

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-152698

(43)Date of publication of application : 23.05.2003

(51)Int.Cl.

H04L 9/08
H04H 1/00
H04L 9/16
H04N 7/08
H04N 7/081
H04N 7/167

(21)Application number : 2001-349539

(71)Applicant : NIPPON HOSO KYOKAI <NHK>

(22)Date of filing : 15.11.2001

(72)Inventor : NISHIMOTO TOMONARI

KURIOKA TATSUYA

UEHARA TOSHIHIRO

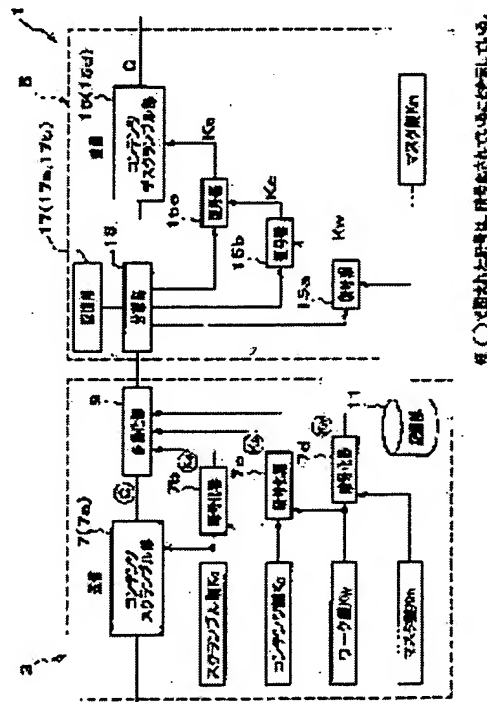
NANBA SEIICHI

OKUDA HARUO

(54) CONTENTS UTILIZATION CONTROL TRANSMITTING METHOD, CONTENTS UTILIZATION CONTROL RECEIVING METHOD, CONTENTS UTILIZATION CONTROL TRANSMITTING DEVICE, CONTENTS UTILIZATION CONTROL RECEIVING DEVICE, CONTENTS UTILIZATION CONTROL TRANSMITTING PROGRAM AND CONTENTS UTILIZATION CONTROL RECEIVING PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a contents utilization control transmitting method, receiving method, contents utilization control transmitting device, receiving device, contents utilization control transmitting program and receiving program in which the illegal utilization of contents can be prevented even when a receiver on a receiving side is illegally altered or illegally produced. SOLUTION: A system is composed of a contents utilization control transmitting device 3 for transmitting encrypted contents in which contents are encrypted, reproduction order control information for controlling the reproduction order of the relevant encrypted contents and viewing control information for controlling viewing of the relevant encrypted contents and a contents utilization control receiving device 5 for receiving such information, the transmitting device 3 is provided with a contents scramble part 7, a multiplexing part 9 and a storage part 11, and the receiving device 5 is provided with a demultiplexing part 13, a contents descramble part 15 and a storage part 17.



LEGAL STATUS

[Date of request for examination]

09.04.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application]

converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-152698

(P2003-152698A)

(43) 公開日 平成15年5月23日 (2003.5.23)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
H 0 4 L	9/08	H 0 4 H 1/00	F 5 C 0 6 3
H 0 4 H	1/00	H 0 4 L 9/00	6 0 1 B 5 C 0 6 4
H 0 4 L	9/16	H 0 4 N 7/08	Z 5 J 1 0 4
H 0 4 N	7/08	7/167	Z
7/081		H 0 4 L 9/00	6 4 3

審査請求 未請求 請求項の数15 O L (全 26 頁) 最終頁に続く

(21) 出願番号 特願2001-349539(P2001-349539)

(22) 出願日 平成13年11月15日 (2001.11.15)

(71) 出願人 000004352

日本放送協会

東京都渋谷区神南2丁目2番1号

(72) 発明者 西本 友成

東京都世田谷区砦一丁目10番11号 日本放送協会 放送技術研究所内

(72) 発明者 栗岡 辰弥

東京都世田谷区砦一丁目10番11号 日本放送協会 放送技術研究所内

(74) 代理人 100064414

弁理士 磯野 道造

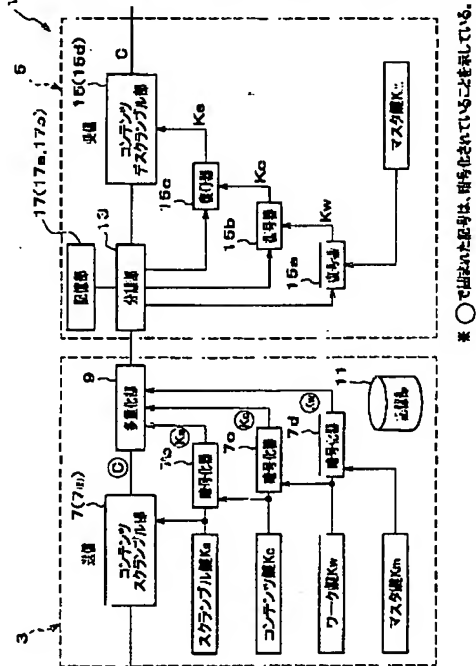
最終頁に続く

(54) 【発明の名称】 コンテンツ利用制御送信方法、コンテンツ利用制御受信方法およびコンテンツ利用制御送信装置、コンテンツ利用制御受信装置ならびにコンテンツ利用制御送信プログラム、コンテンツ利用

(57) 【要約】

【課題】 受信側の受信機が不正に改造されたり不正に製造されたものであっても、コンテンツの不正利用を防止することができるコンテンツ利用制御送信方法、受信方法、コンテンツ利用制御送信装置、受信装置、コンテンツ利用制御送信プログラム、受信プログラムを提供する。

【解決手段】 コンテンツを暗号化した暗号化コンテンツと、当該暗号化コンテンツの再生順序を制御する再生順序制御情報および当該暗号化コンテンツの視聴を制御する視聴制御情報と、を送信するコンテンツ利用制御送信装置3、これらの情報を受信するコンテンツ利用制御受信装置5によって構成し、送信装置3は、コンテンツスクランブル部7と多重化部9と記憶部11とを備え、受信装置5は、分離部13とコンテンツデスクランブル部15と記憶部17とを備えた。



【特許請求の範囲】

【請求項1】 デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの利用を制御する利用制御情報とを送信するコンテンツ利用制御送信方法であって、

経過時間に伴って変更されるスクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化ステップと、

共通鍵暗号化方式に供される共通鍵により、少なくとも前記利用制御情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化ステップと、

前記暗号化コンテンツ、前記暗号化関連情報を多重化し多重暗号コンテンツとする多重化ステップと、

この多重化ステップで多重化された多重暗号コンテンツを送信する多重暗号コンテンツ送信ステップと、を含むことを特徴とするコンテンツ利用制御送信方法。

【請求項2】 前記利用制御情報は、当該暗号化コンテンツの再生順序を制御する再生順序制御情報と、当該暗号化コンテンツの視聴を制御する視聴制御情報との少なくとも一方の情報を含んでいることを特徴とする請求項1に記載のコンテンツ利用制御送信方法。

【請求項3】 デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの再生順序を制御する再生順序制御情報および当該暗号化コンテンツの視聴を制御する視聴制御情報と、を送信するコンテンツ利用制御送信方法であって、

経過時間に伴って変更されるスクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化ステップと、

前記コンテンツ毎に設けられたコンテンツ鍵により、少なくとも前記再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化ステップと、

前記コンテンツの継続時間を越えて保持されるワーク鍵により、少なくとも前記視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化し暗号化コンテンツ鍵関連情報とするコンテンツ鍵関連情報暗号化ステップと、

受信側に共通に備えられるマスター鍵により、少なくとも前記ワーク鍵を含むワーク鍵に関するワーク鍵関連情報を暗号化し暗号化ワーク鍵関連情報とするワーク鍵関連情報暗号化ステップと、

前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報を多重化した多重暗号コンテンツとする多重化ステップと、

この多重化ステップで多重化された多重暗号コンテンツを送信する多重暗号コンテンツ送信ステップと、を含むことを特徴とするコンテンツ利用情報送信方法。

【請求項4】 経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、共通鍵暗号化方式に供される共通鍵により、少なくとも当該暗号化コンテンツの利用を制御する利用制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報とを送信側で多重化した多重暗号コンテンツを受信するコンテンツ利用制御受信方法であって、

前記多重暗号コンテンツを受信する多重暗号コンテンツ受信ステップと、

この多重暗号コンテンツ受信ステップで受信した多重暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報に分離する多重暗号コンテンツ分離ステップと、

この多重暗号コンテンツ分離ステップで分離された暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化利用制御情報を、前記共通鍵により復号する暗号化利用制御情報復号ステップと、

この暗号化利用制御情報復号ステップで復号された利用制御情報に基づいて、前記スクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号ステップと、を含むことを特徴とするコンテンツ利用制御受信方法。

【請求項5】 経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、前記コンテンツ毎に設けられたコンテンツ鍵により少なくとも当該暗号化コンテンツの再生順序を制御する再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報と、前記コンテンツの継続時間を越えて保持されるワーク鍵により少なくとも当該暗号化コンテンツの視聴を制御する視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化した暗号化コンテンツ鍵関連情報と、送信側に共通に備えられるマスター鍵により少なくとも前記ワーク鍵を含むワーク鍵に関するワーク鍵関連情報を暗号化した暗号化ワーク鍵関連情報とを送信側で多重化した多重暗号コンテンツを受信するコンテンツ利用制御受信方法であって、

前記多重暗号コンテンツを受信する多重暗号コンテンツ受信ステップと、

この多重暗号コンテンツ受信ステップで受信した多重暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報に分離する多重暗号コンテンツ分離ステップと、

この多重暗号コンテンツ分離ステップで分離された暗号化ワーク鍵関連情報を前記マスター鍵で復号しワーク鍵を得る暗号化ワーク鍵関連情報復号ステップと、この暗号化ワーク鍵関連情報復号ステップで得られたワ

ーク鍵で暗号化コンテンツ鍵関連情報に含まれている暗号化コンテンツ鍵および暗号化視聴制御情報を復号しコンテンツ鍵および視聴制御情報を得る暗号化コンテンツ鍵関連情報復号ステップと、

この暗号化コンテンツ鍵関連情報復号ステップで復号された視聴制御情報に基づいて、前記暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化再生順序制御情報を復号しスクランブル鍵および再生順序制御情報を得る暗号化関連情報復号ステップと、

この暗号化関連情報復号ステップで復号された再生順序制御情報に基づいて、復号されたスクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号ステップと、を含むことを特徴とするコンテンツ利用制御受信方法。

【請求項6】 デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの利用を制御する利用制御情報とを送信するコンテンツ利用制御送信装置であって、

経過時間に伴って変更されるスクランブル鍵を生成するスクランブル鍵生成手段と、

共通鍵暗号化方式に供される共通鍵を記憶する記憶手段と、

前記スクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化手段と、

前記共通鍵により、少なくとも前記利用制御情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化手段と、

前記暗号化コンテンツ、前記暗号化関連情報を多重化し多重暗号コンテンツとする多重化手段と、

この多重化手段で多重化された多重暗号コンテンツを送信する多重暗号コンテンツ送信手段と、を備えることを特徴とするコンテンツ利用制御送信装置。

【請求項7】 前記利用制御情報は、当該暗号化コンテンツの再生順序を制御する再生順序制御情報と、当該暗号化コンテンツの視聴を制御する視聴制御情報との少なくとも一方の情報を含んでいることを特徴とする請求項6に記載のコンテンツ利用制御送信装置。

【請求項8】 デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの再生順序を制御する再生順序制御情報および当該暗号化コンテンツの視聴を制御する視聴制御情報と、を送信するコンテンツ利用制御送信装置であって、経過時間に伴って変更されるスクランブル鍵を生成するスクランブル鍵生成手段と、

前記コンテンツ毎に設けられたコンテンツ鍵、前記コンテンツの継続時間を越えて保持されるワーク鍵、受信側に共通に備えられるマスター鍵を記憶する記憶手段と、前記スクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化手段と、前記コンテンツ鍵により、少なくとも前記再生順序制御

情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化手段と、

前記ワーク鍵により、少なくとも前記視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化し暗号化コンテンツ鍵関連情報とするコンテンツ鍵関連情報暗号化手段と、

前記マスター鍵により、少なくとも前記ワーク鍵を含むワーク鍵に関するワーク鍵関連情報を暗号化し暗号化ワーク鍵関連情報とするワーク鍵関連情報暗号化手段と、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報を多重化した多重暗号コンテンツとする多重化手段と、

この多重化手段で多重化された多重暗号コンテンツを送信する多重暗号コンテンツ送信手段と、を備えることを特徴とするコンテンツ利用制御送信装置。

【請求項9】 経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、共通鍵暗号化方式に供される共通鍵により、少なくとも当該暗号化コンテンツの利用を制御する利用制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報とを送信側で多重化した多重暗号コンテンツを受信するコンテンツ利用制御受信装置であって、

前記多重暗号コンテンツを受信する多重暗号コンテンツ受信手段と、

この多重暗号コンテンツ受信手段で受信した多重暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報に分離する多重暗号コンテンツ分離手段と、

この多重暗号コンテンツ分離手段で分離された暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化利用制御情報を、前記共通鍵により復号する暗号化利用制御情報復号手段と、

この暗号化利用制御情報復号手段で復号された利用制御情報に基づいて、復号されたスクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号手段と、を備えることを特徴とするコンテンツ利用制御受信装置。

【請求項10】 経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、前記コンテンツ毎に設けられたコンテンツ鍵により少なくとも当該暗号化コンテンツの再生順序を制御する再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報と、前記コンテンツの継続時間を越えて保持されるワーク鍵により少なくとも当該暗号化コンテンツの視聴を制御する視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化した暗号化コンテンツ鍵関連情報と、送信側に共通に備えられるマスター鍵により少なくとも前記ワーク鍵を含む

ワーク鍵に関するワーク鍵関連情報を暗号化した暗号化ワーク鍵関連情報とを送信側で多重化した多重化暗号コンテンツを受信するコンテンツ利用制御受信装置であって、

前記多重化暗号コンテンツを受信する多重化暗号コンテンツ受信手段と、

この多重化暗号コンテンツ受信手段で受信した多重化暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報に分離する多重化暗号コンテンツ分離手段と、

この多重化暗号コンテンツ分離手段で分離された暗号化ワーク鍵関連情報を前記マスター鍵で復号しワーク鍵を得る暗号化ワーク鍵関連情報復号手段と、

この暗号化ワーク鍵関連情報復号手段で得られたワーク鍵で暗号化コンテンツ鍵関連情報に含まれている暗号化コンテンツ鍵および暗号化視聴制御情報を復号しコンテンツ鍵および視聴制御情報を得る暗号化コンテンツ鍵関連情報復号手段と、

この暗号化コンテンツ鍵関連情報復号手段で復号された視聴制御情報に基づいて、前記暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化再生順序制御情報を復号しスクランブル鍵および再生順序制御情報を得る暗号化関連情報復号手段と、

この暗号化関連情報復号手段で復号された再生順序制御情報に基づいて、復号されたスクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号手段と、を備えることを特徴とするコンテンツ利用制御受信装置。

【請求項11】 デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの利用を制御する利用制御情報とを送信するコンテンツ利用制御送信装置を、

経過時間に伴って変更されるスクランブル鍵を生成するスクランブル鍵生成手段、

共通鍵暗号化方式に供される共通鍵を記憶する記憶手段、

前記スクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化手段、

前記共通鍵により、少なくとも前記利用制御情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化手段、

前記暗号化コンテンツ、前記暗号化関連情報を多重化し多重暗号コンテンツとする多重化手段、

この多重化手段で多重化された多重化暗号コンテンツを送信する多重化暗号コンテンツ送信手段、として機能させることを特徴とするコンテンツ利用制御送信プログラム。

【請求項12】 請求項11に記載のコンテンツ利用制御送信プログラムにおいて、前記利用制御情報は、当該

暗号化コンテンツの再生順序を制御する再生順序制御情報と、当該暗号化コンテンツの視聴を制御する視聴制御情報との少なくとも一方の情報を含んでいることを特徴とするコンテンツ利用制御送信プログラム。

【請求項13】 デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの再生順序を制御する再生順序制御情報および当該暗号化コンテンツの視聴を制御する視聴制御情報と、を送信するコンテンツ利用制御送信装置を、経過時間に伴って変更されるスクランブル鍵を生成するスクランブル鍵生成手段、

前記コンテンツ毎に設けられたコンテンツ鍵、前記コンテンツの継続時間を越えて保持されるワーク鍵、受信側に共通に備えられるマスター鍵を記憶する記憶手段、

前記スクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化手段、

前記コンテンツ鍵により、少なくとも前記再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化手段、

前記ワーク鍵により、少なくとも前記視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化し暗号化コンテンツ鍵関連情報とするコンテンツ鍵関連情報暗号化手段、

前記マスター鍵により、少なくとも前記ワーク鍵を含むワーク鍵に関するワーク鍵関連情報を暗号化し暗号化ワーク鍵関連情報とするワーク鍵関連情報暗号化手段、

前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報を多重化した多重化暗号コンテンツとする多重化手段、この多重化手段で多重化された多重化暗号コンテンツを送信する多重化暗号コンテンツ送信手段、として機能させることを特徴とするコンテンツ利用制御送信プログラム。

【請求項14】 経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、共通鍵暗号化方式に供される共通鍵により、少なくとも当該暗号化コンテンツの利用を制御する利用制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報とを送信側で多重化した多重化暗号コンテンツを受信するコンテンツ利用制御受信装置を、

前記多重化暗号コンテンツを受信する多重化暗号コンテンツ受信手段、

この多重化暗号コンテンツ受信手段で受信した多重化暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報に分離する多重化暗号コンテンツ分離手段、

この多重化暗号コンテンツ分離手段で分離された暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化利用制御情報を、前記共通鍵により復号する暗号化利用制御情報復号手段、

この暗号化利用制御情報復号手段で復号された利用制御情報に基づいて、復号されたスクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号手段、として機能させることを特徴とするコンテンツ利用制御受信プログラム。

【請求項15】 経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、前記コンテンツ毎に設けられたコンテンツ鍵により少なくとも当該暗号化コンテンツの再生順序を制御する再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報と、前記コンテンツの継続時間を越えて保持されるワーク鍵により少なくとも当該暗号化コンテンツの視聴を制御する視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化した暗号化コンテンツ鍵関連情報と、送信側に共通に備えられるマスター鍵により少なくとも前記ワーク鍵を含むワーク鍵に関するワーク鍵関連情報を暗号化した暗号化ワーク鍵関連情報とを送信側で多重化した多重化暗号コンテンツを受信するコンテンツ利用制御受信装置を、前記多重化暗号コンテンツを受信する多重化暗号コンテンツ受信手段、

この多重化暗号コンテンツ受信手段で受信した多重化暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報に分離する多重化暗号コンテンツ分離手段、

この多重化暗号コンテンツ分離手段で分離された暗号化ワーク鍵関連情報を前記マスター鍵で復号しワーク鍵を得る暗号化ワーク鍵関連情報復号手段、

この暗号化ワーク鍵関連情報復号手段で得られたワーク鍵で暗号化コンテンツ鍵関連情報に含まれている暗号化コンテンツ鍵および暗号化視聴制御情報を復号しコンテンツ鍵および視聴制御情報を得る暗号化コンテンツ鍵関連情報復号手段、

この暗号化コンテンツ鍵関連情報復号手段で復号された視聴制御情報に基づいて、前記暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化再生順序制御情報を復号しスクランブル鍵および再生順序制御情報を得る暗号化関連情報復号手段、

この暗号化関連情報復号手段で復号された再生順序制御情報に基づいて、復号されたスクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号手段、として機能させることを特徴とするコンテンツ利用制御受信プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタル放送におけるコンテンツの利用を制御するコンテンツ利用制御送信方法、コンテンツ利用制御受信方法およびコンテンツ

利用制御送信装置、コンテンツ利用制御受信装置ならびにコンテンツ利用制御送信プログラム、コンテンツ利用制御受信プログラムに関する。

【0002】

【従来の技術】近年、デジタル放送におけるコンテンツ（デジタルコンテンツ）を、受信側で大容量のハードディスク等のランダムアクセス可能な蓄積装置に蓄積し、利用（再生、編集等）するサービス（コンテンツの視聴）が想定されている。このサービスは、ランダムアクセス可能な蓄積装置にコンテンツを蓄積させ、コンテンツのあるシーンのみ（視聴者が所望するシーン）をノンリニアに再生させることにより、実現可能になるものである。

【0003】また、デジタル放送におけるコンテンツには、コンテンツ中に各シーンに対応するメタデータ（コンテンツに関する情報：特にコンテンツ（番組）内の各シーンの見出しに相当する番組内インデックス）が付されており、このメタデータが付されたコンテンツが送信側から送信され、受信側で当該メタデータをコンテンツ検索（コンテンツの特定シーンの検索）に利用されることが想定されている。

【0004】

【発明が解決しようとする課題】ところが、ランダムアクセス可能な蓄積装置にコンテンツが蓄積されることによって実現されるサービスは、受信者側の視聴者に対して便利なサービスである一方、送信者側の放送局（コンテンツ制作者）にとっては、放送局（コンテンツ制作者）の意図しないコンテンツの利用が行われる（コンテンツの不正利用）可能性がある。例えば、コンテンツ中に含まれているCM等のコンテンツの一部が意図的にスキップされ（削除され）視聴される恐れがある。また、送信側でコンテンツに付されたメタデータを、受信側で悪意を持った視聴者が不正に改ざんしたり、別のメタデータを付してコンテンツを利用する（コンテンツの不正利用）恐れがある。

【0005】従来、このようなコンテンツの不正利用を防止するための方策（防止策）として、コンテンツ中のシーンやCMをスキップをさせない為の制御信号を、コンテンツと併せて（多重化して）送信側から送信し、受信側の受信機で当該制御信号に従って、当該受信機を動作させることで、コンテンツを視聴することが想定されている。

【0006】しかしながら、従来のコンテンツの不正利用の防止策では、送信側で多重化された制御信号に従って、受信側の受信機が制御されることが前提となっているが、受信側の受信機が不正に改造されていたり、不正に製造されたものであった場合、送信側で多重化された制御信号は有効に機能しないことが想定される。

【0007】そこで、本発明の目的は前記した従来の技術が有する課題を解消し、受信側の受信機が不正に改造

されたり不正に製造されたものであっても、コンテンツの不正利用を防止することができるコンテンツ利用制御送信方法、コンテンツ利用制御受信方法およびコンテンツ利用制御送信装置、コンテンツ利用制御受信装置ならびにコンテンツ利用制御送信プログラム、コンテンツ利用制御受信プログラムを提供することにある。

【0008】

【課題を解決するための手段】前記した目的を達成するため、以下に示す構成とした。請求項1記載のコンテンツ利用制御送信方法は、デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの利用を制御する利用制御情報とを送信するコンテンツ利用制御送信方法であって、経過時間に伴って変更されるスクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化ステップと、共通鍵暗号化方式に供される共通鍵により、少なくとも前記利用制御情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化ステップと、前記暗号化コンテンツ、前記暗号化関連情報を多重化し多重暗号コンテンツとする多重化ステップと、この多重化ステップで多重化された多重暗号コンテンツを送信する多重暗号コンテンツ送信ステップと、を含むことを特徴とする。

【0009】この方法では、まず、コンテンツ暗号化ステップにおいて、経過時間に伴って変更されるスクランブル鍵によってコンテンツが暗号化され暗号化コンテンツとされる。一方、スクランブル鍵を含む関連情報と利用制御情報とが、共通鍵暗号化方式に供される共通鍵によって暗号化され暗号化関連情報とされる。そして、これらが多重化ステップにおいて多重化され多重暗号コンテンツとされ、多重暗号コンテンツ送信ステップで送信される。

【0010】また、請求項2記載のコンテンツ利用制御送信方法は、請求項1に記載のコンテンツ利用制御送信方法において、前記利用制御情報は、当該暗号化コンテンツの再生順序を制御する再生順序制御情報と、当該暗号化コンテンツの視聴を制御する視聴制御情報との少なくとも一方の情報を含んでいることを特徴とする。

【0011】この方法では、利用制御情報が再生順序制御情報と視聴制御情報との少なくとも一方の情報を含んでいるので、受信側でコンテンツを利用するときに、この情報に従って、送信側の意図するようにコンテンツの利用制御がなされる。

【0012】また、請求項3記載のコンテンツ利用制御送信方法は、デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの再生順序を制御する再生順序制御情報および当該暗号化コンテンツの視聴を制御する視聴制御情報と、を送信するコンテンツ利用制御送信方法であって、経過時間に伴って変更されるスクランブル鍵により、前記コンテ

ンツを暗号化して暗号化コンテンツとするコンテンツ暗号化ステップと、前記コンテンツ毎に設けられたコンテンツ鍵により、少なくとも前記再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化ステップと、前記コンテンツの継続時間を越えて保持されるワーク鍵により、少なくとも前記視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化し暗号化コンテンツ鍵関連情報とするコンテンツ鍵関連情報暗号化ステップと、受信側に共通に備えられるマスター鍵により、少なくとも前記ワーク鍵を含むワーク鍵に関するワーク鍵関連情報を暗号化し暗号化ワーク鍵関連情報とするワーク鍵関連情報暗号化ステップと、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報を多重化した多重暗号コンテンツとする多重化ステップと、この多重化ステップで多重化された多重暗号コンテンツを送信する多重暗号コンテンツ送信ステップと、を含むことを特徴とする。

【0013】この方法では、まず、コンテンツ暗号化ステップにおいて、経過時間に伴って変更されるスクランブル鍵によって、コンテンツが暗号化され暗号化コンテンツとされる。次に、関連情報暗号化ステップにおいて、コンテンツ毎に設けられたコンテンツ鍵によって、少なくとも再生順序制御情報およびスクランブル鍵を含む関連情報が暗号化され暗号化関連情報とされる。また、コンテンツ鍵関連情報暗号化ステップにおいて、コンテンツの継続時間を越えて保持されるワーク鍵によって、少なくとも視聴制御情報およびコンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報が暗号化され暗号化コンテンツ鍵関連情報とされる。さらに、ワーク鍵関連情報暗号化ステップにおいて、受信側に共通に備えられるマスター鍵によって、少なくともワーク鍵を含むワーク鍵に関するワーク鍵関連情報が暗号化され暗号化ワーク鍵関連情報とされる。そして、多重化ステップにおいて、暗号化コンテンツ、暗号化関連情報、暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報が多重化され多重暗号コンテンツとされ、多重暗号コンテンツ送信ステップで、この多重暗号コンテンツが送信される。

【0014】さらに、請求項4記載のコンテンツ利用制御受信方法は、経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、共通鍵暗号化方式に供される共通鍵により、少なくとも当該暗号化コンテンツの利用を制御する利用制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報とを送信側で多重化した多重暗号コンテンツを受信するコンテンツ利用制御受信方法であって、前記多重暗号コンテンツを受信する多重暗号コンテンツ受信ステップと、この多重

化暗号コンテンツ受信ステップで受信した多重化暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報に分離する多重化暗号コンテンツ分離ステップと、この多重化暗号コンテンツ分離ステップで分離された暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化利用制御情報を、前記共通鍵により復号する暗号化利用制御情報復号ステップと、この暗号化利用制御情報復号ステップで復号された利用制御情報に基づいて、前記スクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号ステップと、を含むことを特徴とする。

【0015】この方法では、まず、多重化暗号コンテンツ受信ステップにおいて、暗号化コンテンツと暗号化関連情報とが送信側で多重化された多重化暗号コンテンツが受信される。そして、多重化暗号コンテンツ分離ステップにおいて、多重化暗号コンテンツが暗号化コンテンツと暗号化関連情報とに分離され、暗号化利用制御情報復号ステップにおいて、暗号化スクランブル鍵および暗号化利用制御情報が復号される。そしてさらに、暗号化コンテンツ復号ステップにおいて、復号された利用制御情報に基づいて暗号化コンテンツが復号される。

【0016】また、請求項5記載のコンテンツ利用制御受信方法は、経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、前記コンテンツ毎に設けられたコンテンツ鍵により少なくとも当該暗号化コンテンツの再生順序を制御する再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報と、前記コンテンツの継続時間を越えて保持されるワーク鍵により少なくとも当該暗号化コンテンツの視聴を制御する視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化した暗号化コンテンツ鍵関連情報と、送信側に共通に備えられるマスター鍵により少なくとも前記ワーク鍵を含むワーク鍵に関するワーク鍵関連情報を暗号化した暗号化ワーク鍵関連情報とを送信側で多重化した多重化暗号コンテンツを受信するコンテンツ利用制御受信方法であって、前記多重化暗号コンテンツを受信する多重化暗号コンテンツ受信ステップと、この多重化暗号コンテンツ受信ステップで受信した多重化暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報に分離する多重化暗号コンテンツ分離ステップと、この多重化暗号コンテンツ分離ステップで分離された暗号化ワーク鍵関連情報を前記マスター鍵で復号しワーク鍵を得る暗号化ワーク鍵関連情報復号ステップと、この暗号化ワーク鍵関連情報復号ステップで得られたワーク鍵で暗号化コンテンツ鍵関連情報に含まれている暗号化コンテンツ鍵および暗号化視聴制御情報を復号しコンテンツ鍵および視聴制御情報を得る暗号化コンテンツ鍵関連情報復号ステ

ップと、この暗号化コンテンツ鍵関連情報復号ステップで復号された視聴制御情報に基づいて、前記暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化再生順序制御情報を復号しスクランブル鍵および再生順序制御情報を得る暗号化関連情報復号ステップと、この暗号化関連情報復号ステップで復号された再生順序制御情報に基づいて、復号されたスクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号ステップと、を含むことを特徴とする。

【0017】この方法では、まず、多重化暗号コンテンツ受信ステップにおいて、暗号化コンテンツ、暗号化関連情報、暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報が送信側で多重化された多重化暗号コンテンツが受信される。そして、多重化暗号コンテンツ分離ステップにおいて、これらが分離される。そしてまた、ここで分離された暗号化ワーク鍵関連情報がマスター鍵で復号されワーク鍵が得られ、暗号化コンテンツ鍵関連情報復号ステップにおいて、得られたワーク鍵で暗号化コンテンツ鍵および暗号化視聴制御情報が復号され、コンテンツ鍵および視聴制御情報が得られる。この視聴制御情報に基づいて、暗号化関連情報復号ステップにおいて、暗号化スクランブル鍵および暗号化再生順序制御情報が復号され、この再生順序制御情報に基づいて、暗号化コンテンツ復号ステップにおいて、スクランブル鍵で暗号化コンテンツが復号される。

【0018】或いはまた、請求項6記載のコンテンツ利用制御送信装置は、デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの利用を制御する利用制御情報とを送信するコンテンツ利用制御送信装置であって、経過時間に伴って変更されるスクランブル鍵を生成するスクランブル鍵生成手段と、共通鍵暗号化方式に供される共通鍵を記憶する記憶手段と、前記スクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化手段と、前記共通鍵により、少なくとも前記利用制御情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化手段と、前記暗号化コンテンツ、前記暗号化関連情報を多重化し多重暗号コンテンツとする多重化手段と、この多重化手段で多重化された多重化暗号コンテンツを送信する多重化暗号コンテンツ送信手段と、を備えることを特徴とする。

【0019】かかる構成によれば、まず、スクランブル鍵生成手段で生成されたスクランブル鍵を用いて、コンテンツ暗号化手段でコンテンツが暗号化され暗号化コンテンツとされる。一方、関連情報暗号化手段で、スクランブル鍵を含む関連情報と利用制御情報とが、記憶手段に記憶されている共通鍵によって暗号化され暗号化関連情報とされる。そして、これらが多重化手段で多重化され多重化暗号コンテンツとされ、多重化暗号コンテンツ送信手段で送信される。

【0020】また、請求項7記載のコンテンツ利用制御送信装置は、請求項6に記載のコンテンツ利用制御送信装置において、前記利用制御情報は、当該暗号化コンテンツの再生順序を制御する再生順序制御情報と、当該暗号化コンテンツの視聴を制御する視聴制御情報との少なくとも一方の情報を含んでいることを特徴とする。

【0021】かかる構成によれば、利用制御情報が再生順序制御情報と視聴制御情報との少なくとも一方の情報を含んでいるので、受信側でコンテンツを利用するときに、この情報に従って、送信側の意図するようにコンテンツの利用制御がなされる。

【0022】また、請求項8記載のコンテンツ利用制御送信装置は、デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの再生順序を制御する再生順序制御情報および当該暗号化コンテンツの視聴を制御する視聴制御情報と、を送信するコンテンツ利用制御送信装置であって、経過時間に伴って変更されるスクランブル鍵を生成するスクランブル鍵生成手段と、前記コンテンツ毎に設けられたコンテンツ鍵、前記コンテンツの継続時間を越えて保持されるワーク鍵、受信側に共通に備えられるマスター鍵を記憶する記憶手段と、前記スクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化手段と、前記コンテンツ鍵により、少なくとも前記再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化手段と、前記ワーク鍵により、少なくとも前記視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化し暗号化コンテンツ鍵関連情報とするコンテンツ鍵関連情報暗号化手段と、前記マスター鍵により、少なくとも前記ワーク鍵を含むワーク鍵に関するワーク鍵関連情報を暗号化し暗号化ワーク鍵関連情報とするワーク鍵関連情報暗号化手段と、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報を多重化した多重化暗号コンテンツとする多重化手段と、この多重化手段で多重化された多重化暗号コンテンツを送信する多重化暗号コンテンツ送信手段と、を備えることを特徴とする。

【0023】かかる構成によれば、まず、スクランブル鍵生成手段で生成されたスクランブル鍵を用いて、コンテンツ暗号化手段でコンテンツが暗号化され暗号化コンテンツとされる。一方、関連情報暗号化手段で、記憶手段に記憶されているコンテンツ鍵によって、少なくとも再生順序制御情報およびスクランブル鍵を含む関連情報が暗号化し暗号化関連情報とされる。また、コンテンツ鍵関連情報暗号化手段で、記憶手段に記憶されているワーク鍵によって、少なくとも視聴制御情報およびコンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報が暗号化され暗号化コンテンツ鍵関連情報とされ

る。さらに、ワーク鍵関連情報暗号化手段で、マスター鍵によって、少なくともワーク鍵を含むワーク鍵に関するワーク鍵関連情報が暗号化され暗号化ワーク鍵関連情報とされる。そして、多重化手段で、これらが多重化暗号コンテンツとされ、多重化暗号コンテンツ送信手段で送信される。

【0024】さらに、請求項9記載のコンテンツ利用制御受信装置は、経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、共通鍵暗号化方式に供される共通鍵により、少なくとも当該暗号化コンテンツの利用を制御する利用制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報とを送信側で多重化した多重化暗号コンテンツを受信するコンテンツ利用制御受信装置であって、前記多重化暗号コンテンツを受信する多重化暗号コンテンツ受信手段と、この多重化暗号コンテンツ受信手段で受信した多重化暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報に分離する多重化暗号コンテンツ分離手段と、この多重化暗号コンテンツ分離手段で分離された暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化利用制御情報を、前記共通鍵により復号する暗号化利用制御情報復号手段と、この暗号化利用制御情報復号手段で復号された利用制御情報に基づいて、復号されたスクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号手段と、を備えることを特徴とする。

【0025】かかる構成によれば、まず、多重化暗号コンテンツ受信手段で、暗号化コンテンツと暗号化関連情報とが送信側で多重化された多重化暗号コンテンツが受信される。そして、多重化暗号コンテンツ分離手段で、多重化暗号コンテンツが暗号化コンテンツと暗号化関連情報とに分離され、暗号化利用制御情報復号手段で、暗号化スクランブル鍵および暗号化利用制御情報が復号される。そしてさらに、暗号化コンテンツ復号手段で、復号された利用制御情報に基づいて暗号化コンテンツが復号される。

【0026】また、請求項10記載のコンテンツ利用制御受信装置は、経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、前記コンテンツ毎に設けられたコンテンツ鍵により少なくとも当該暗号化コンテンツの再生順序を制御する再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報と、前記コンテンツの継続時間を越えて保持されるワーク鍵により少なくとも当該暗号化コンテンツの視聴を制御する視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化した暗号化コンテンツ鍵関連情報と、送信側に共通に備えられるマスター鍵により少なくとも前記ワーク鍵を含むワーク鍵に関するワーク鍵関連情報を暗号化した暗号化

ワーク鍵関連情報とを送信側で多重化した多重化暗号コンテンツを受信するコンテンツ利用制御受信装置であって、前記多重化暗号コンテンツを受信する多重化暗号コンテンツ受信手段と、この多重化暗号コンテンツ受信手段で受信した多重化暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報に分離する多重化暗号コンテンツ分離手段と、この多重化暗号コンテンツ分離手段で分離された暗号化ワーク鍵関連情報を前記マスター鍵で復号しワーク鍵を得る暗号化ワーク鍵関連情報復号手段と、この暗号化ワーク鍵関連情報復号手段で得られたワーク鍵で暗号化コンテンツ鍵関連情報に含まれている暗号化コンテンツ鍵および暗号化視聴制御情報を復号しコンテンツ鍵および視聴制御情報を得る暗号化コンテンツ鍵関連情報復号手段と、この暗号化コンテンツ鍵関連情報復号手段で復号された視聴制御情報に基づいて、前記暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化再生順序制御情報を復号しスクランブル鍵および再生順序制御情報を得る暗号化関連情報復号手段と、この暗号化関連情報復号手段で復号された再生順序制御情報に基づいて、復号されたスクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号手段と、を備えることを特徴とする。

【0027】かかる構成によれば、まず、多重化暗号コンテンツ受信手段で、暗号化コンテンツ、暗号化関連情報、暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報が送信側で多重化された多重化暗号コンテンツが受信される。そして、多重化暗号コンテンツ分離手段で、これらが分離される。そしてまた、ここで分離された暗号化ワーク鍵関連情報がマスター鍵で復号されワーク鍵が得られ、暗号化コンテンツ鍵関連情報復号手段で、得られたワーク鍵で暗号化コンテンツ鍵および暗号化視聴制御情報が復号され、コンテンツ鍵および視聴制御情報が得られる。この視聴制御情報に基づいて、暗号化関連情報復号手段で、暗号化スクランブル鍵および暗号化再生順序制御情報が復号され、この再生順序制御情報に基づいて、暗号化コンテンツ復号手段で、スクランブル鍵で暗号化コンテンツが復号される。

【0028】さらにまた、請求項11記載のコンテンツ利用制御送信プログラムは、デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの利用を制御する利用制御情報とを送信するコンテンツ利用制御送信装置を、以下に示す手段として機能させることを特徴とする。コンテンツ利用制御送信装置を機能させる手段は、経過時間に伴って変更されるスクランブル鍵を生成するスクランブル鍵生成手段、共通鍵暗号化方式に供される共通鍵を記憶する記憶手段、前記スクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化手段、前記共通鍵により、少なくとも前記利用制御情報お

よび前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化手段、前記暗号化コンテンツ、前記暗号化関連情報を多重化し多重暗号コンテンツとする多重化手段、この多重化手段で多重化された多重化暗号コンテンツを送信する多重化暗号コンテンツ送信手段、である。

【0029】かかる構成によれば、まず、スクランブル鍵生成手段で生成されたスクランブル鍵を用いて、コンテンツ暗号化手段でコンテンツが暗号化され暗号化コンテンツとされる。一方、関連情報暗号化手段で、スクランブル鍵を含む関連情報と利用制御情報とが、記憶手段に記憶されている共通鍵によって暗号化され暗号化関連情報とされる。そして、これらが多重化手段で多重化され多重化暗号コンテンツとされ、多重化暗号コンテンツ送信手段で送信される。

【0030】また、請求項12記載のコンテンツ利用制御送信プログラムは、請求項11に記載のコンテンツ利用制御送信プログラムにおいて、前記利用制御情報は、当該暗号化コンテンツの再生順序を制御する再生順序制御情報と、当該暗号化コンテンツの視聴を制御する視聴制御情報との少なくとも一方の情報を含んでいることを特徴とする。

【0031】かかる構成によれば、利用制御情報が再生順序制御情報と視聴制御情報との少なくとも一方の情報を含んでいるので、受信側でコンテンツを利用するときに、この情報に従って、送信側の意図するようにコンテンツの利用制御がなされる。

【0032】また、請求項13記載のコンテンツ利用制御送信プログラムは、デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの再生順序を制御する再生順序制御情報および当該暗号化コンテンツの視聴を制御する視聴制御情報と、を送信するコンテンツ利用制御送信装置を、以下に示す手段として機能させることを特徴とする。コンテンツ利用制御装置を機能させる手段は、経過時間に伴って変更されるスクランブル鍵を生成するスクランブル鍵生成手段、前記コンテンツ毎に設けられたコンテンツ鍵、前記コンテンツの継続時間を越えて保持されるワーク鍵、受信側に共通に備えられるマスター鍵を記憶する記憶手段、前記スクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化手段、前記コンテンツ鍵により、少なくとも前記再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化手段、前記ワーク鍵により、少なくとも前記視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化し暗号化コンテンツ鍵関連情報とするコンテンツ鍵関連情報暗号化手段、前記マスター鍵により、少なくとも前記ワーク鍵を含むワーク鍵に関するワーク鍵関連情報を暗号化し暗号化ワーク鍵関連情

報とするワーク鍵関連情報暗号化手段、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報を多重化した多重化暗号コンテンツとする多重化手段、この多重化手段で多重化された多重化暗号コンテンツを送信する多重化暗号コンテンツ送信手段、である。

【0033】かかる構成によれば、まず、スクランブル鍵生成手段で生成されたスクランブル鍵を用いて、コンテンツ暗号化手段でコンテンツが暗号化され暗号化コンテンツとされる。一方、関連情報暗号化手段で、記憶手段に記憶されているコンテンツ鍵によって、少なくとも再生順序制御情報およびスクランブル鍵を含む関連情報が暗号化し暗号化関連情報とされる。また、コンテンツ鍵関連情報暗号化手段で、記憶手段に記憶されているワーク鍵によって、少なくとも視聴制御情報およびコンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報が暗号化され暗号化コンテンツ鍵関連情報とされる。さらに、ワーク鍵関連情報暗号化手段で、マスター鍵によって、少なくともワーク鍵を含むワーク鍵に関するワーク鍵関連情報が暗号化され暗号化ワーク鍵関連情報とされる。そして、多重化手段で、これらが多重化暗号コンテンツとされ、多重化暗号コンテンツ送信手段で送信される。

【0034】さらに、請求項14記載のコンテンツ利用制御受信プログラムは、経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、共通鍵暗号化方式に供される共通鍵により、少なくとも当該暗号化コンテンツの利用を制御する利用制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報とを送信側で多重化した多重化暗号コンテンツを受信するコンテンツ利用制御受信装置を、以下に示す手段として機能させることを特徴とする。コンテンツ利用制御受信装置を機能させる手段は、前記多重化暗号コンテンツを受信する多重化暗号コンテンツ受信手段、この多重化暗号コンテンツ受信手段で受信した多重化暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報に分離する多重化暗号コンテンツ分離手段、この多重化暗号コンテンツ分離手段で分離された暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化利用制御情報を、前記共通鍵により復号する暗号化利用制御情報復号手段、この暗号化利用制御情報復号手段で復号された利用制御情報に基づいて、復号されたスクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号手段、である。

【0035】かかる構成によれば、まず、多重化暗号コンテンツ受信手段で、暗号化コンテンツと暗号化関連情報とが送信側で多重化された多重化暗号コンテンツが受信される。そして、多重化暗号コンテンツ分離手段で、多重化暗号コンテンツが暗号化コンテンツと暗号化関連

情報とに分離され、暗号化利用制御情報復号手段で、暗号化スクランブル鍵および暗号化利用制御情報が復号される。そしてさらに、暗号化コンテンツ復号手段で、復号された利用制御情報に基づいて暗号化コンテンツが復号される。

【0036】また、請求項15記載のコンテンツ利用制御受信プログラムは、経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、前記コンテンツ毎に設けられたコンテンツ鍵により少なくとも当該暗号化コンテンツの再生順序を制御する再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報と、前記コンテンツの継続時間を越えて保持されるワーク鍵により少なくとも当該暗号化コンテンツの視聴を制御する視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化した暗号化コンテンツ鍵関連情報と、送信側に共通に備えられるマスター鍵により少なくとも前記ワーク鍵を含むワーク鍵に関するワーク鍵関連情報を暗号化した暗号化ワーク鍵関連情報とを送信側で多重化した多重化暗号コンテンツを受信するコンテンツ利用制御受信装置を、以下に示す手段として機能させることを特徴とする。コンテンツ利用制御受信装置を機能させる手段は、前記多重化暗号コンテンツを受信する多重化暗号コンテンツ受信手段、この多重化暗号コンテンツ受信手段で受信した多重化暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化ワーク鍵関連情報に分離する多重化暗号コンテンツ分離手段、この多重化暗号コンテンツ分離手段で分離された暗号化ワーク鍵関連情報を前記マスター鍵で復号しワーク鍵を得る暗号化ワーク鍵関連情報復号手段、この暗号化ワーク鍵関連情報復号手段で得られたワーク鍵で暗号化コンテンツ鍵関連情報に含まれている暗号化コンテンツ鍵および暗号化視聴制御情報を復号しコンテンツ鍵および視聴制御情報を得る暗号化コンテンツ鍵関連情報復号手段、この暗号化コンテンツ鍵関連情報復号手段で復号された視聴制御情報に基づいて、前記暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化再生順序制御情報を復号しスクランブル鍵および再生順序制御情報を得る暗号化関連情報復号手段、この暗号化関連情報復号手段で復号された再生順序制御情報に基づいて、復号されたスクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号手段、である。

【0037】かかる構成によれば、まず、多重化暗号コンテンツ受信手段で、暗号化コンテンツ、暗号化関連情報、暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報が送信側で多重化された多重化暗号コンテンツが受信される。そして、多重化暗号コンテンツ分離手段で、これらが分離される。そしてまた、ここで分離された暗

号化ワーク鍵関連情報がマスター鍵で復号されワーク鍵が得られ、暗号化コンテンツ鍵関連情報復号手段で、得られたワーク鍵で暗号化コンテンツ鍵および暗号化視聴制御情報が復号され、コンテンツ鍵および視聴制御情報が得られる。この視聴制御情報に基づいて、暗号化関連情報復号手段で、暗号化スクランブル鍵および暗号化再生順序制御情報が復号され、この再生順序制御情報に基づいて、暗号化コンテンツ復号手段で、スクランブル鍵で暗号化コンテンツが復号される。

【0038】

【発明の実施の形態】以下、本発明の一実施形態を図面に基いて詳細に説明する。

(コンテンツ利用制御システム(コンテンツ利用制御送信装置およびコンテンツ利用制御受信装置))図1にコンテンツ利用制御システムのブロック図を示す。この図1に示すように、コンテンツ利用制御システム1は、コンテンツ利用制御送信装置3とコンテンツ利用制御受信装置5とを備えて構成されている。

【0039】コンテンツ利用制御システム1は、デジタル放送におけるコンテンツを暗号化して受信側で当該暗号化したコンテンツの利用(再生、編集等)を制御(制限)する情報(利用制御情報)と共に送信することで、受信側でのコンテンツの利用を制御可能にするシステムである。

【0040】(コンテンツ利用制御送信装置の構成)まず、コンテンツ利用制御送信装置3について説明する。コンテンツ利用制御送信装置3は、コンテンツスクランブル部7と、多重化部9と、記憶部11とを備えて構成されている。コンテンツ利用制御送信装置3は、映像・音声データからなるコンテンツを暗号化して、受信側のコンテンツ利用制御受信装置5に送信するものであって、受信側と共通に備えられるマスター鍵を利用して(このため、共通鍵暗号化方式とされる)当該コンテンツを暗号化し送信するものである。

【0041】コンテンツスクランブル部7は、まず、図示を省略したスクランブル鍵生成部で生成されたスクランブル鍵Ksを用いて、送信するコンテンツを暗号化し暗号化コンテンツとする(暗号化器7a)。次に、記憶部11に記憶されているコンテンツ鍵Kcを用いて、少なくともスクランブル鍵Ksおよび再生手順番号(再生順序制御情報:利用制御情報の1つ)を含む関連情報を暗号化し暗号化関連情報とする(暗号化器7b)。つまり、暗号化されたスクランブル鍵Ksは、MPEG-2多重化方式のセクション形式でパケット化される。このパケット化の具体的な方式の例として、ARIBの限定受信方式規格(STD-B25)に記載されたECM(Entitlement Control Message)形式が利用でき、同規格と同様な方式でパケット化し送出することができる。

【0042】また、コンテンツスクランブル部7は、記

憶部11に記憶されているワーク鍵Kwを用いて、少なくともコンテンツ鍵Kcおよび視聴制御フラグ(視聴制御情報:利用制御情報の1つ)を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化し暗号化コンテンツ鍵関連情報とする(暗号化器7c)。さらに、記憶部11に記憶されているマスター鍵Kmを用いて、少なくともワーク鍵Kwを含むワーク鍵Kwに関するワーク鍵関連情報を暗号化し暗号化ワーク鍵関連情報とする(暗号化器7d)。

【0043】なお、コンテンツをコンテンツ利用制御受信装置5でリアルタイムに視聴させる場合には、コンテンツ鍵Kc(暗号化コンテンツ鍵Kc)の送出が、当該コンテンツを送出する所定時間前から開始され、コンテンツが送出されている間、コンテンツ鍵Kcが所定時間間隔で繰り返し送出され、コンテンツ送出終了後、コンテンツ鍵Kcの送出も終了される。一方、コンテンツをコンテンツ利用制御受信装置5の記憶部(後記する)に記憶後、記憶したコンテンツを再生させて視聴する場合には、記憶部にスクランブルしたままのコンテンツ(暗号化コンテンツ)を記憶させておき、当該コンテンツの視聴を許可するとき(送信側で制御)に、当該コンテンツに対応するコンテンツ鍵Kcが送出される。

【0044】また、コンテンツ利用制御送信装置3のコンテンツスクランブル部7と請求項に記載した構成との対応関係を補足すると、コンテンツスクランブル部7(7a)がコンテンツ暗号化手段に、暗号化器7bが関連情報暗号化手段に、暗号化器7cがコンテンツ鍵関連情報暗号化手段に、暗号化器7dがワーク鍵関連情報暗号化手段に相当するものである。

【0045】多重化部9は、コンテンツスクランブル部7で暗号化された暗号化コンテンツと、暗号化関連情報と、暗号化コンテンツ鍵関連情報と、暗号化ワーク鍵関連情報とをトランスポートストリームとして多重化して多重化暗号コンテンツを生成し、受信側に送出するものである。なお、この多重化部9が請求項に記載した多重化手段と多重化暗号コンテンツ送信手段に相当するものである。

【0046】記憶部11は、コンテンツ鍵Kc、ワーク鍵Kw、マスター鍵Kmを記憶しておくものであり、それぞれ、コンテンツ鍵Kcデータベース、ワーク鍵Kwデータベース、マスター鍵Kmデータベースといった形式で記憶(格納)されている。

【0047】ここで、各暗号鍵、利用制御情報について補足説明しておく。スクランブル鍵Ksは、経過時間(数秒単位)に伴って変更される暗号鍵であり、コンテンツ鍵Kcは、コンテンツ毎に設定される暗号鍵である。また、ワーク鍵Kwは、コンテンツの継続時間を越えて保持される暗号鍵であり、マスター鍵Kmは、コンテンツ利用制御受信装置5に備えられている送受信間で共通の暗号鍵である。そして、このマスター鍵Kmは、

コンテンツ利用制御受信装置5(後記するセキュリティモジュール)各々に割り当てられた固有の鍵である。なお、このマスター鍵K_mは、予めセキュリティモジュール内に書き込まれて、受信側(コンテンツ利用制御受信装置5に付属させて)に配布されている。

【0048】そして、視聴制御フラグ(視聴制御情報)は、コンテンツの視聴をフラグのオンオフで制御するもので、フラグがオンの場合、受信側で暗号化スクランブルが復号後、再生手順番号に基づいてコンテンツの視聴が決定される。フラグがオフの場合、受信側で即座に暗号化スクランブル鍵が復号されてコンテンツの視聴が許可される。さらに、再生手順番号(再生順序制御情報)は、コンテンツの視聴順序を制御する情報であり、詳細は後記する。

【0049】(コンテンツ利用制御受信装置の構成)次に、コンテンツ利用制御受信装置5について説明する。コンテンツ利用制御受信装置5は、分離部13と、コンテンツデスクランブル部15と、記憶部17とを備えて構成されている。コンテンツ利用制御受信装置5は、送信側のコンテンツ利用制御送信装置3で暗号化され、多重化された多重化暗号コンテンツを受信し、この多重化暗号コンテンツに含まれている利用制御情報(視聴制御フラグ、再生手順番号)に従って、多重化暗号コンテンツを復号し、コンテンツを視聴可能にするものである。

【0050】分離部13は、送信側のコンテンツ利用制御送信装置3から送信された多重化暗号コンテンツを受信すると共に、受信した多重化暗号コンテンツを、暗号化コンテンツ、暗号化関連情報、暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報に分離するものである。この分離部13が請求項に記載した多重化暗号コンテンツ受信手段と多重化暗号コンテンツ分離手段とに相当するものである。

【0051】コンテンツデスクランブル部15は、4つの復号器(後記するセキュリティモジュールSM)を備えて構成されており、分離部13で分離された暗号化コンテンツ、暗号化関連情報、暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報を復号するものであって、まず、暗号化ワーク鍵関連情報がマスター鍵により復号されワーク鍵が得られる(復号器15a)。

【0052】そして、このワーク鍵により暗号化コンテンツ鍵関連情報が復号されコンテンツ鍵および視聴制御フラグが得られ(復号器15b)、この視聴制御フラグ(オンorオフ)に基づいて、コンテンツ鍵により暗号化関連情報が復号され、スクランブル鍵のみ、または、スクランブル鍵および再生手順番号が得られる(復号器15c)。

【0053】さらに、この再生手順番号に基づいて、スクランブル鍵により暗号化コンテンツが復号され、コンテンツが得られる(コンテンツデスクランブル部15(復号器15d))。このコンテンツデスクランブル部

15が、請求項に記載した多重暗号コンテンツ復号手段に相当するものである。記憶部17は、コンテンツ利用制御受信装置5本体に一体的に備えられているメモリ部17aと、記憶媒体に情報を記憶させる記憶媒体取扱手段17bとを備えて構成されている。

【0054】また、コンテンツ利用制御受信装置5には、この図1において図示を省略したセキュリティモジュールSM1が備えられている。このセキュリティモジュールSM1は、少なくとも復号器15a~15cを備え、マスター鍵K_mが保持されるものであって、外部より読み出し不可能なICカード等から構成されている。またこのセキュリティモジュールSM1には、図示を省略した記憶部Nが備えられており、この記憶部Nは、再生手順番号の数値(利用制御情報の1つ)を記憶するカウンタに相当するものである。なお、この記憶部Nに記憶される再生手順番号の数値は、初期値として1が記憶されており、コンテンツ鍵関連情報に含まれるコンテンツIDおよびコンテンツ鍵K_cが変更されるたびに数値の再設定(初期値1に設定)が行われる。

【0055】(ワーク鍵K_wの共有化について)ここで、ある複数のコンテンツ利用制御受信装置5において、ワーク鍵K_wを共有させたい場合を想定して説明する。まず、送信側のコンテンツ利用制御送信装置3は、該当するコンテンツ利用制御受信装置5のマスター鍵K_mを、記憶部11のマスター鍵K_mデータベースより読み出し、このマスター鍵K_mによりワーク鍵K_wを共通鍵暗号化方式の暗号化器7dで暗号化する。この暗号化されたワーク鍵K_w(暗号化ワーク鍵K_w)を含む関連情報を、例えば、MPEG-2多重化方式のセクション形式でパケット化し、個別情報として、多重化部9で暗号化した暗号化コンテンツと併せてトランスポートストリームとして多重化する。

【0056】このパケット化の例として、ARIBの限定受信方式規格(STD-B25)に記載されたEMM(Entitlement Management Message)形式が利用可能である。そして、受信側のコンテンツ利用制御受信装置5では、分離部13で受信したMPEG-2トランスポートストリームから、EMMを取り出し、マスター鍵K_mを用いて、復号器15aで復号し、ワーク鍵K_wを得る。

【0057】この動作を、各コンテンツ利用制御受信装置5に対して繰り返し実行し、これにより、ワーク鍵K_wを送受信間で共有させることができる。また、得られたワーク鍵K_wは、セキュリティモジュールSM(図1には図示せず)に保存される。そして、複数のコンテンツ利用制御受信装置5間で共有化された当該ワーク鍵K_wは、ワーク鍵K_w自体の安全性を維持するために、例えば1ヶ月や1年といった単位で更新される。また、このワーク鍵K_wは放送帯域の空いた帯域を利用して、コンテンツとは独立に順次送信される。

【0058】(ファイルフォーマットの例)次に、送信側のコンテンツ利用制御送信装置3から送信されるファイルのフォーマット例を図2を参照して説明する。コンテンツ利用制御送信装置3から送信されるファイルのフォーマットには、スクランブル鍵関連情報S(共通情報S)、コンテンツ鍵関連情報C(共通情報C)、ワーク鍵関連情報W(個別情報W)の3種類がある。

【0059】スクランブル鍵関連情報S(共通情報S)は、スクランブル鍵の送出に用いられる番組情報であり、事業者ID、コンテンツID、スクランブル鍵Ks、再生手順番号等から構成されている。事業者IDは放送事業者に割り当てられた識別子であり、コンテンツIDは、コンテンツ毎にユニークに、或いは、所定の条件(例えば、再放送番組を同一IDとするか別のIDとするか等の条件)に基づいて、割り当てられた識別子である。そして、スクランブル鍵Ksは、コンテンツIDに対応するコンテンツ鍵Kcによって暗号化される。また、再生手順番号は、受信側でコンテンツの再生順序を規定するものである。

【0060】コンテンツ鍵関連情報C(共通情報C)は、コンテンツ鍵Kcの送出に用いられる共通の情報であり、事業者ID、ワーク鍵ID、コンテンツID、コンテンツ鍵Kc、有効期限、記憶場所指定、視聴制御フラグ等から構成されている。事業者IDは放送事業者に割り当てられた識別子であり、ワーク鍵IDはワーク鍵を識別する識別子であり、コンテンツIDは、コンテンツ毎にユニークに、割り当てられた識別子である。これらのうち少なくともコンテンツ鍵Kcは、ワーク鍵IDに対応するワーク鍵によって暗号化されている。

【0061】また、有効期限は、コンテンツ鍵Kcの有効期限を示すものであり、記憶場所指定は、受信したコンテンツ鍵をコンテンツ利用制御受信装置5のどこに記憶させるかを予め送信側で指定するものである。視聴制御フラグは、コンテンツの視聴をフラグのオンオフで制御するもので、フラグがオンの場合、受信側で暗号化スクランブルが復号後、再生手順番号に基づいてコンテンツの視聴が決定されるものである。

【0062】ワーク鍵関連情報W(個別情報W)は、ワーク鍵Kwの送出に用いられる個別情報であり、事業者ID、カードID、更新番号、有効期限、ワーク鍵ID、ワーク鍵等から構成されている。事業者IDは、放送事業者或いはその特定の集合(グループ)等に割り当てられた識別子であり、カードIDは、セキュリティモジュールSM毎に割り当てられた識別子であり、更新番号は、ワーク鍵Kwのバージョンを示す番号であり、有効期限は、ワーク鍵Kwの有効期限を示すものである。そして、ワーク鍵Kwは、カードIDに対応するマスター鍵Kmによって暗号化されている。

【0063】(コンテンツ利用制御受信装置とセキュリティモジュールとの関係(構成))次に、図3を参照し

て、コンテンツ利用制御システム1におけるコンテンツ利用制御受信装置5とセキュリティモジュールSM1との関係を説明する。コンテンツ利用制御受信装置5は、受信したストリーム(多重暗号コンテンツ)からワーク鍵Kwやコンテンツ鍵Kcを含む関連情報を分離するKw・Kc関連情報分離部13aと、暗号化コンテンツを記憶する記憶部17aと、スクランブル鍵Ksを含む関連情報を分離するKs関連情報分離部13bと、コンテンツをデスクランブルするコンテンツデスクランブル部15と、コンテンツ利用制御受信装置5とセキュリティモジュールSM1との通信を行うインターフェース等から構成されている。

【0064】セキュリティモジュールSM1は、マスター鍵Kmを備え、4つの復号器(19a~19d)と、1つの暗号化器21と、スクランブル鍵Ksを送出させる送出部23と、この送出部23を制御する送出制御部25と、状況に応じて入力される複数の情報を制御するソフトウェアスイッチS/Wとを備えて構成されている。このソフトウェアスイッチS/Wに、入力される情報数は2個であり、この情報数に対応してa1、a2のスイッチが備えられており、スイッチa1がリアルタイムにコンテンツを視聴する場合、スイッチa2が記憶再生視聴する場合に対応している。

【0065】Kw・Kc関連情報分離部13aで、多重化暗号コンテンツから暗号化ワーク鍵関連情報を抽出し、この暗号化ワーク鍵関連情報に記述されているカードIDと、セキュリティモジュールSM1(この実施の形態ではICカード)のカードIDとが一致する場合、ワーク鍵Kw、ワーク鍵ID、更新番号、有効期限、事業者IDとが含まれている暗号化ワーク鍵関連情報をセキュリティモジュールSM1に入力する。セキュリティモジュールSM1では、入力された暗号化されているワーク鍵Kwをマスター鍵Kmで復号し、ワーク鍵Kwを得て(復号器19a)、このワーク鍵Kwは、事業者ID、更新番号、有効期限、ワーク鍵IDとに対応させて、セキュリティモジュールSM1内で保持される。

【0066】一方、Kw・Kc関連情報分離部13aにおいて、暗号化コンテンツ鍵関連情報を抽出し、ワーク鍵IDと、暗号化されているコンテンツ鍵Kc、事業者ID、有効期限、コンテンツIDとが含まれている暗号化コンテンツ鍵関連情報をセキュリティモジュールSM1に入力する。セキュリティモジュールSM1では、暗号化コンテンツ鍵関連情報をワーク鍵IDに対応するワーク鍵Kwを用いて復号し、コンテンツ鍵Kcを得る(復号器19b)。

【0067】(暗号化コンテンツの再生例(リアルタイム視聴))次に、図3に図示したコンテンツ利用制御受信装置5およびセキュリティモジュールSM1を用いて、送信されているコンテンツ(リアルタイム)を視聴する場合について説明する。リアルタイムにコンテンツ

を視聴する場合であるので、予め、セキュリティモジュールSM1のソフトウェアスイッチS/Wをa1に切り替えておく。

【0068】Kw・Kc関連情報分離部13aの出力は、Ks関連情報分離部13bに入力される。Ks関連情報分離部13bでは、関連情報Sを抽出し、コンテンツIDと暗号化されたスクランブル鍵Ksを含む関連情報SをセキュリティモジュールSM1に入力する。セキュリティモジュールSM1では、関連情報SをコンテンツIDに対応するコンテンツ鍵Kcを用いて復号し、スクランブル鍵Ksおよび再生手順番号を得る(復号器19d)。そして、得られた再生手順番号を送出制御部25に入力し、この再生手順番号が入力された送出手順番号25は、再生手順番号に基づいて、送出手順番号25を制御し、復号器19dで得られたスクランブル鍵Ksをコンテンツ利用制御受信装置5に送出する。このスクランブル鍵Ksを受信したコンテンツ利用制御受信装置5のコンテンツデスクランブル部15は、スクランブル鍵Ksを用いて暗号化コンテンツを復号し、コンテンツを出力する。

【0069】(暗号化コンテンツの再生例(記憶再生視聴))次に、図3に図示したコンテンツ利用制御受信装置5およびセキュリティモジュールSM1を用いて、記憶部17aに記憶したコンテンツを視聴する場合について説明する。記憶部17aに記憶させたコンテンツを視聴する場合であるので、予め、セキュリティモジュールSM1のソフトウェアスイッチS/Wをa2に切り替えておく。

【0070】暗号化コンテンツはそのまま(スクランブル化されたまま)、暗号化されたスクランブル鍵を含む暗号化関連情報(関連情報S)と共に、コンテンツIDと対応されて、記憶部17aに記憶されている。一方、Kw・Kc関連情報分離部13aにおいて、暗号化コンテンツ鍵関連情報(コンテンツ鍵関連情報C)を抽出し、抽出した、暗号化されたコンテンツ鍵を含む暗号化コンテンツ鍵関連情報をセキュリティモジュールSM1に入力する。そして、復号器19bで復号されたコンテンツ鍵を、マスター鍵を用いて暗号化する(暗号化器21)。この暗号化されたコンテンツ鍵Kcをコンテンツ利用制御受信装置5に出力し、記憶部17aに記憶されている暗号化コンテンツと対応させて記憶する。

【0071】そして、記憶部17aに記憶されているコンテンツを再生するときには、デスクランブルするコンテンツに対応する、暗号化されたコンテンツ鍵Kcを記憶部17aから読み出して、セキュリティモジュールSM1に入力する。セキュリティモジュールSM1では、入力された、暗号化されているコンテンツ鍵Kcをマスター鍵Kmにより、復号しコンテンツ鍵Kcを得る(復号器19c)。また一方、再生されたコンテンツは、Ks関連情報分離部13bに入力され、暗号化関連情報

(関連情報S)を抽出し、暗号化されているスクランブル鍵Ksを含む暗号化関連情報(関連情報S)をセキュリティモジュールSM1に入力する。

【0072】セキュリティモジュールSM1では、入力された、暗号化されているスクランブル鍵Ksを含む暗号化関連情報を、復号器19cで復号されたコンテンツ鍵Kcで復号し、スクランブル鍵Ksおよび再生手順番号を得る(復号器19d)。再生手順番号を送出制御部25に入力し、送出手順番号25は得られた再生手順番号に基づいて、送出手順番号25を制御し、コンテンツ利用制御受信装置5にスクランブル鍵Ksを送出する。コンテンツ利用制御受信装置5では、受信したスクランブル鍵Ksを用いて、コンテンツデスクランブル部15で暗号化コンテンツがデスクランブルされ、コンテンツが出力される。

【0073】また、コンテンツ利用制御受信装置5にホームネットワーク等を介して、記憶装置(図示せず)が接続されている場合には、Ks関連情報分離部13bに入力される前に、ストリーム(多重化暗号コンテンツの一部)が、ホームネットワーク等を介して、コンテンツ利用制御受信装置5以外の記憶装置に記憶される。

【0074】このとき、暗号化コンテンツおよび暗号化関連情報と併せて、マスター鍵Kmで暗号化した再暗号化コンテンツ鍵を記憶装置に記憶させる。暗号化コンテンツの再生時には、記憶装置で再生された信号(スクランブルされたままのコンテンツ信号)がコンテンツ利用制御受信装置5のKs関連情報分離部13bにホームネットワークを介して入力されると共に、コンテンツ利用制御受信装置5を介して再暗号化コンテンツ鍵がセキュリティモジュールSM1に入力され、復号器19cで再暗号化コンテンツ鍵が復号され、復号器19dでスクランブル鍵Ksが得られ、コンテンツがデスクランブルされる。

【0075】(コンテンツ利用制御受信装置に入力されるストリーム(多重化暗号コンテンツ)に対する各鍵の対応関係、再生手順番号の例)次に、図4を参照して、コンテンツ利用制御受信装置5に入力されるストリーム(多重化暗号コンテンツ:コンテンツの各シーン)に対する、スクランブル鍵Ks、コンテンツ鍵Kc、の対応関係を説明する。ここでは、コンテンツがリアルタイムに視聴される場合を想定しており、コンテンツの中身をシーンA、シーンB、シーンC、シーンD、シーンEといった具合に時間軸方向に区切った場合について説明する。例えば、コンテンツをあるドラマであるとする、シーンAはドラマのプロローグに、シーンBはCMに、シーンCはドラマの中核に、シーンDはCMに、シーンEはドラマのエピローグに相当する。

【0076】これらの各シーンA～Eをスクランブルしているスクランブル鍵Ks(Ks11～Ks5n)および再生手順番号はスクランブル鍵関連情報に含まれてい

る。シーンAの間は1秒程度の時間でスクランブル鍵Ks11からスクランブル鍵Ks1nに順次変更され、スクランブル鍵Ks11からスクランブル鍵Ks1nには同じ再生手順番号1が付されている。

【0077】また、シーンBの間は、1秒程度の時間でスクランブル鍵Ks21からスクランブル鍵Ks2nに順次変更され、スクランブル鍵Ks21からスクランブル鍵Ks2nには複数の再生手順番号2、3、4、5が付されている。シーンCの間は1秒程度の時間でスクランブル鍵Ks31からスクランブル鍵Ks3nに順次変更され、スクランブル鍵Ks31からスクランブル鍵Ks3nには同じ再生手順番号6が付されている。

【0078】さらに、シーンDの間は、1秒程度の時間でスクランブル鍵Ks41からスクランブル鍵Ks4nに順次変更され、スクランブル鍵Ks41からスクランブル鍵Ks4nには複数の再生手順番号7、8、9が付されている。シーンEの間は1秒程度の時間でスクランブル鍵Ks51からスクランブル鍵Ks5nに順次変更され、スクランブル鍵Ks51からスクランブル鍵Ks5nには同じ再生手順番号10が付されている。

【0079】なお、多重化暗号コンテンツには、コンテンツ鍵関連情報C1（暗号化されている）が含まれており、このコンテンツ鍵関連情報C1には、コンテンツ鍵Kc、視聴制御フラグ（オン）が含まれている。このコンテンツ鍵Kcはコンテンツの各シーンすなわちシーンAからシーンDまで、同一のものが用いられる。また、視聴制御フラグがオンであれば、再生手順番号に基づいてコンテンツ利用制御受信装置5にスクランブル鍵Ksが送出され、視聴制御フラグがオフであれば、再生手順番号に拘わらずコンテンツ利用制御受信装置5にスクランブル鍵Ksが送出される。

【0080】（コンテンツの視聴制御（利用制御）の例1）ここで、図3、図4を参照して、コンテンツに付されている再生手順番号に基づいたコンテンツ（シーンA～E）の視聴制御を説明する。セキュリティモジュールSM1の送出制御部25は、現時点で復号しているスクランブル鍵Ksの再生手順番号と、次のスクランブル鍵Ksの再生手順番号とを比較し、現時点で復号しているスクランブル鍵Ksの再生手順番号と次のスクランブル鍵Ksの再生手順番号とが同一か、現時点で復号しているスクランブル鍵Ksの再生手順番号に1を加算したものと等しい場合に、復号したスクランブル鍵Ksを送出部23からコンテンツ利用制御受信装置5に送出させる。

【0081】いずれの場合にも該当しない際には、送出制御部25は、コンテンツの再生順序が制限されている旨のエラーメッセージ（エラー信号）を送出部23からコンテンツ利用制御受信装置5に送出させる。これにより、スクランブル鍵KsがセキュリティモジュールSM1からコンテンツ利用制御受信装置5に送出された場合

には、図4中の再生例Aに示したように当該装置5で暗号化コンテンツがコンテンツデスクランブル15でデスクランブルされ、コンテンツを視聴することができる。

【0082】また、コンテンツが記憶部17に記憶されている際に、図4中の再生例A1に示したように、シーンAの一部分シーンA1、シーンCの一部分シーンC1、シーンEの一部分シーンE1を順次ノンリニアに再生しようとする場合を説明する。この場合、シーンA1では、再生手順番号が1であるので、送出制御部25は、スクランブル鍵Ks（Ks11からKs1nのいずれか）を送出部23からコンテンツ利用制御受信装置5に送出させ、コンテンツ利用制御受信装置5では、受信したスクランブル鍵Ksによりコンテンツ（シーンA1）をデスクランブルする。

【0083】ところが、次のシーンC1では、再生手順番号が6であるので、送出制御部25は、スクランブル鍵Ks（Ks31からKs3nのいずれか）を送出部23からコンテンツ利用制御受信装置5に送出させない。このため、コンテンツ利用制御受信装置5では、コンテンツ（シーンC1）をデスクランブルすることができない。それゆえ、再生手順番号2、3、4、5が付されているシーンBをデスクランブルしてからシーンC1をデスクランブルする必要が生じる。同様に、再生手順番号7、8、9が付されているシーンDをデスクランブルしてからでないでシーンE1をデスクランブルすることができない。

【0084】つまり、コンテンツ利用制御受信装置5において、シーンAからシーンCにノンリニアに再生しようとする場合には、シーンCを再生する際の再生手順番号が不明であるので、再生手順番号を得るために、必ず、シーンBを再生する必要がある。これにより、シーンBであるCMをスキップさせてコンテンツを視聴することを防止することができる。すなわち、コンテンツ利用制御受信装置5のユーザのコンテンツの視聴を送信側で制御することができる。

【0085】（コンテンツの視聴制御（利用制御；再生手順番号の利用の仕方）の例2）また、スクランブル鍵関連情報に含まれる再生手順番号の利用の仕方について補足説明する。例えば、コンテンツ（シーンA～E）がドラマである場合、シーンAからシーンDまでは、各シーンA～Dに同じ再生手順番号1を付しておき、シーンE（ドラマのクライマックス）のみ、再生手順番号を数秒間隔で増加させるように再生手順番号2、3、4、5、6と付しておけば、シーンAからシーンDまでは、コンテンツ利用制御受信装置5（当該装置5に接続される表示装置（図示せず））で自由に視聴できるが、コンテンツ利用制御受信装置5のユーザがシーンEのみ最初に再生させて視聴することを防止することができる。

【0086】或いは、ドラマ（コンテンツ）に出演している出演者のインタビューの映像をシーンEに含ませて

おき、シーンAからシーンDまですべて視聴したユーザのみシーンEを視聴できるといった視聴制御も可能である。つまり、シーンE（コンテンツの最後）に視聴者が最も視聴したいシーンを含ませておくことで、それ以前のシーンAからシーンD（CM等を含む）を視聴者に積極的に視聴させることができる。

【0087】（コンテンツの視聴制御（利用制御）の例3）一方、コンテンツ鍵関連情報に含まれている視聴制御フラグがオフの場合には、図5中の再生例B1に示したように、再生手順番号に関係なく、コンテンツを再生することができる。つまり、再生例Bに示したようなシーンAからシーンEまでの連続再生ではなく、シーンAの一部であるシーンA1と、シーンCの一部であるシーンC1と、シーンEの一部であるシーンE1とを順次連続再生することができる。

【0088】これによれば、例えば、無料コンテンツを放送する無料放送時には、コンテンツ鍵関連情報に含まれている視聴制御フラグをオンにしたコンテンツ鍵Kcにより、コンテンツ利用制御受信装置5のユーザにコンテンツを視聴させる。すると、当該ユーザは、コンテンツに含まれているCM等をスキップさせることができない。この際に、当該ユーザがコンテンツに含まれているCM等のスキップを望む場合、通信回線等を用いて、一定の料金を送信側のコンテンツ利用制御送信装置3を所有する放送事業者に支払う契約をすると、当該装置3から視聴制御フラグをオフにしたコンテンツ鍵Kc（コンテンツ鍵関連情報）が当該通信回線を介して送信されるようにすることも可能である。この視聴制御フラグをオフにしたコンテンツ鍵Kcを入手したユーザは視聴制限なく（当該コンテンツに限り）コンテンツを利用することができる。このため、無料放送時においても、送信側の放送事業者の意図するコンテンツの視聴（CM等をスキップさせない等の利用制御）を受信側のユーザに行わせることができる。

【0089】（コンテンツの視聴制御（利用制御；複数のワーク鍵）の例4）さらにまた、コンテンツを送信する送信側の放送事業者は、予め、複数の種類のワーク鍵Kw（Kw1、Kw2・・・）を準備しておく（コンテンツ利用制御送信装置3の記憶部11のワーク鍵データベースに記憶）。そして、放送事業者は無料でコンテンツを受信しているコンテンツ利用制御受信装置5のユーザには、ワーク鍵Kw1を、放送事業者に定額料金を支払ってコンテンツを受信しているコンテンツ利用制御受信装置5のユーザには、ワーク鍵Kw2を、セキュリティモジュールSM1に記憶させて、それぞれのユーザに配布しておく。

【0090】その後、コンテンツ利用制御送信装置3からコンテンツ送出時（多重化暗号コンテンツ）に、ワーク鍵Kw1で暗号化されているコンテンツ鍵関連情報（視聴制御フラグはオン）およびワーク鍵Kw2で暗号

化されているコンテンツ鍵関連情報（視聴制御フラグはオフ）を併せて送出すれば、ユーザとの契約状況に応じた視聴制御を行うことができる。

【0091】また、図4、図5に示したコンテンツの視聴制御（利用制御）の例では、再生手順番号を1ずつ増加させたが、シーンAからシーンDまでは、図4、図5に示したように再生手順番号を付しておき、シーンEのみ再生手順番号20を付しておくと、送信側で送出されるコンテンツ鍵Kcを含むコンテンツ鍵関連情報（視聴制御フラグはオン）では、シーンEを視聴することができない。この際に、当該ユーザがシーンEの視聴を望む場合、通信回線等を用いて、一定の料金を送信側のコンテンツ利用制御送信装置3を所有する放送事業者に支払う契約をすると、当該装置3から視聴制御フラグをオフにしたコンテンツ鍵Kc（コンテンツ鍵関連情報）が当該通信回線を介して送信されるようにすることも可能である。

【0092】（コンテンツ利用制御受信装置の動作1（記憶後のコンテンツ、ノンリニア再生））図6を参照して、コンテンツ利用制御受信装置5の記憶部17に記憶されているコンテンツを視聴制御する際の動作を説明する。なお、このシーケンスチャートでは、コンテンツがファイルとして記憶部17に記憶されており、当該コンテンツが冒頭から再生されることを想定している。

【0093】コンテンツ利用制御受信装置5の分離部13で多重化暗号コンテンツが分離され暗号化コンテンツ鍵関連情報（コンテンツ鍵Kcを含む）が得られ（S1）、この暗号化コンテンツ鍵関連情報がセキュリティモジュールSM1に送出される。この暗号化コンテンツ鍵関連情報を受信したセキュリティモジュールSM1では、当該暗号化コンテンツ鍵関連情報に含まれているコンテンツ鍵Kcおよび視聴制御フラグが復号される（S2）。

【0094】そして、復号された視聴制御フラグがオンであるかオフであるかが判断され（S3）、復号された視聴制御フラグがオフであると判断された場合には、多重化暗号コンテンツが分離されて得られた暗号化関連情報がコンテンツ利用制御受信装置5からセキュリティモジュールSM1に送出される（S4）。この暗号化関連情報を受信したセキュリティモジュールSM1では、当該暗号化関連情報に含まれている暗号化スクランブル鍵Ksが復号され（S5）、復号されたスクランブル鍵Ksがコンテンツ利用制御受信装置5に送出される（S6）。スクランブル鍵Ksを受信したコンテンツ利用制御受信装置5では、コンテンツデスクランブル部15で、コンテンツ（暗号化コンテンツ）が復号される（S7）。

【0095】S3にて、復号された視聴制御フラグがオンであると判断された場合には、多重化暗号コンテンツが分離されて得られた暗号化関連情報（スクランブル鍵

Ksと再生手順番号を含む)がコンテンツ利用制御受信装置5からセキュリティモジュールSM1に送出される(S8)。この暗号化関連情報を受信したセキュリティモジュールSM1では、当該暗号化関連情報に含まれている暗号化スクランブル鍵Ksおよび再生手順番号が復号される(S9)。

【0096】そして、復号された再生手順番号の数値と記憶部Nに記憶されている数値(初期値は1)とが比較され、再生手順番号の数値が記憶部Nに記憶されている数値n以下かどうか判断される(S10)。比較判断された結果、再生手順番号の数値が記憶部Nに記憶されている数値n以下であると判断された場合には、コンテンツ利用制御受信装置5にスクランブル鍵Ksが送出され(S11)、このスクランブル鍵Ksを受信したコンテンツ利用制御受信装置5では、コンテンツデスクランブル部15で、暗号化コンテンツが復号される(S12)。

【0097】S10にて、再生手順番号の数値が記憶部Nに記憶されている数値n以下であると判断されない場合には、再生手順番号の数値が数値nに1加算した値であるかどうか判断される(S13)。再生手順番号の数値が数値nに1加算した値であると判断されない場合には、スクランブル鍵Ksの送出が中断され、コンテンツ利用制御受信装置5においてエラー処理が行われる(S14)。このエラー処理はセキュリティモジュールSM1がコンテンツ利用制御受信装置5に対して暗号化コンテンツを復号できない旨のエラー番号(エラー情報)を送出することによって実行される。

【0098】S13にて、再生手順番号の数値が数値nに1加算した値であると判断された場合には、この数値nが記憶部Nに記憶され(S15)、コンテンツ利用制御受信装置5にスクランブル鍵Ksが送出され(S11)、このスクランブル鍵Ksを受信したコンテンツ利用制御受信装置5では、コンテンツデスクランブル部15で、暗号化コンテンツが復号される(S12)。

【0099】これらの動作によれば、コンテンツは、暗号化関連情報(スクランブル鍵関連情報)に含まれている再生手順番号(再生順序制御情報;利用制御情報の一つ)に従った場合のみ復号されるので、当該コンテンツに一体的に含まれているCMのスキップ等を防止することができると共に、巻き戻し等により一度視聴した区間(コンテンツの一部)は、自由にノンリニア再生することができる。

【0100】(コンテンツ利用制御受信装置の動作2(記憶後のコンテンツ、再生手順番号順))図7を参照して、コンテンツ利用制御受信装置5の記憶部17に記憶されているコンテンツを視聴制御する際の動作を説明する。なお、このシーケンスチャートでは、コンテンツがファイルとして記憶部17に記憶されており、当該コンテンツが冒頭から再生されることを想定している。

【0101】コンテンツ利用制御受信装置5の分離部13で多重化暗号コンテンツが分離され暗号化コンテンツ鍵関連情報(コンテンツ鍵Kcを含む)が得られ(S21)、この暗号化コンテンツ鍵関連情報がセキュリティモジュールSM1に送出される。この暗号化コンテンツ鍵関連情報を受信したセキュリティモジュールSM1では、当該暗号化コンテンツ鍵関連情報に含まれているコンテンツ鍵Kcおよび視聴制御フラグが復号される(S22)。

【0102】そして、復号された視聴制御フラグがオンであるかオフであるかが判断され(S23)、復号された視聴制御フラグがオフであると判断された場合には、多重化暗号コンテンツが分離されて得られた暗号化関連情報がコンテンツ利用制御受信装置5からセキュリティモジュールSM1に送出される(S24)。この暗号化関連情報を受信したセキュリティモジュールSM1では、当該暗号化関連情報に含まれている暗号化スクランブル鍵Ksが復号され(S25)、復号されたスクランブル鍵Ksがコンテンツ利用制御受信装置5に送出される(S26)。スクランブル鍵Ksを受信したコンテンツ利用制御受信装置5では、コンテンツデスクランブル部15で、暗号化コンテンツが復号される(S27)。

【0103】S23にて、復号された視聴制御フラグがオンであると判断された場合には、多重化暗号コンテンツが分離されて得られた暗号化関連情報がコンテンツ利用制御受信装置5からセキュリティモジュールSM1に送出される(S28)。この暗号化関連情報を受信したセキュリティモジュールSM1では、当該暗号化関連情報に含まれている暗号化スクランブル鍵Ksおよび再生手順番号が復号される(S29)。

【0104】そして、復号された再生手順番号の数値と記憶部Nに記憶されている数値(初期値は1)とが比較され、同じ数値であるかどうか判断される(S30)。比較判断された結果、再生手順番号の数値が記憶部Nに記憶されている数値nと同じであると判断された場合には、コンテンツ利用制御受信装置5にスクランブル鍵Ksが送出され(S31)、このスクランブル鍵Ksを受信したコンテンツ利用制御受信装置5では、コンテンツデスクランブル部15で、暗号化コンテンツが復号される(S32)。

【0105】S30にて、再生手順番号の数値が記憶部Nに記憶されている数値nと同じであると判断されない場合には、再生手順番号の数値が数値n未満か、または再生手順番号の数値が数値nに1加算した値であるかどうか判断される(S33)。再生手順番号の数値が数値n未満か、再生手順番号の数値が数値nに1加算した値であると判断されない場合には、スクランブル鍵Ksの送出が中断され、コンテンツ利用制御受信装置5においてエラー処理が行われる(S34)。このエラー処理はセキュリティモジュールSM1がコンテンツ利用制御

受信装置5に対して暗号化コンテンツを復号できない旨のエラー番号(エラー情報)を送出することによって実行される。

【0106】S33にて、再生手順番号の数値が数値n未満か、再生手順番号の数値がnに1加算した値であると判断された場合には、この数値nが記憶部Nに記憶され(S35)、コンテンツ利用制御受信装置5にスクランブル鍵Ksが送出され(S31)、このスクランブル鍵Ksを受信したコンテンツ利用制御受信装置5では、コンテンツデスクランブル部15で、暗号化コンテンツが復号される(S32)。

【0107】これらの動作によれば、コンテンツは、暗号化関連情報(スクランブル鍵関連情報)に含まれている再生手順番号(再生順序制御情報; 利用制御情報の一つ)に従った場合のみ復号されるので、当該コンテンツに一体的に含まれているCMのスキップ等を防止することができる。また、この動作では、再生手順番号の数値が記憶部Nに記憶されている数値nよりも小さい場合であっても、記憶部Nに再生手順番号を記憶させる手順(S33、S34)を追加している。このため、巻き戻し等により一度視聴した区間(コンテンツの一部)であっても、同様に再生手順番号に従った視聴制限をすることができる。

【0108】(コンテンツ利用制御受信装置の動作3(リアルタイムのコンテンツ))図8を参照して、コンテンツ利用制御受信装置5でリアルタイムに受信しているコンテンツを視聴制御する際の動作を説明する。この動作はリアルタイムに受信しているコンテンツと記憶部17に記憶されたコンテンツの両方を考慮した動作で、放送されているコンテンツを途中から記憶して視聴する場合や、記憶しつつ視聴する際に一部分のコンテンツが記憶できなかったり視聴できなかった場合に対応するための動作である。

【0109】コンテンツ利用制御受信装置5の分離部13で多重化暗号コンテンツが分離され暗号化コンテンツ鍵関連情報(コンテンツ鍵Kcを含む)が得られ(S41)、この暗号化コンテンツ鍵関連情報がセキュリティモジュールSM1に送出される。この暗号化コンテンツ鍵関連情報を受信したセキュリティモジュールSM1では、当該暗号化コンテンツ鍵関連情報に含まれているコンテンツ鍵Kcおよび視聴制御フラグが復号される(S42)。

【0110】そして、復号された視聴制御フラグがオンであるかオフであるかが判断され(S43)、復号された視聴制御フラグがオフであると判断された場合には、多重化暗号コンテンツが分離されて得られた暗号化関連情報がコンテンツ利用制御受信装置5からセキュリティモジュールSM1に送出される(S44)。この暗号化関連情報を受信したセキュリティモジュールSM1では、当該暗号化関連情報に含まれている暗号化スクラン

ブル鍵Ksが復号され(S45)、復号されたスクランブル鍵Ksがコンテンツ利用制御受信装置5に送出される(S46)。スクランブル鍵Ksを受信したコンテンツ利用制御受信装置5では、コンテンツデスクランブル部15で、暗号化コンテンツが復号される(S47)。

【0111】S43にて、復号された視聴制御フラグがオンであると判断された場合には、多重化暗号コンテンツが分離されて得られた暗号化関連情報がコンテンツ利用制御受信装置5からセキュリティモジュールSM1に送出される(S48)。この暗号化関連情報を受信したセキュリティモジュールSM1では、当該暗号化関連情報に含まれている暗号化スクランブル鍵Ksおよび再生手順番号が復号される(S49)。

【0112】そして、最初に受信した再生手順番号の数値を記憶部Nに記憶させておき(S50)、復号された再生手順番号の数値と記憶部Nに記憶されている数値(最初に受信した際の数値)とが比較され、同じ数値であるかどうか判断される(S51)。比較判断された結果、再生手順番号の数値が記憶部Nに記憶されている数値nと同じであると判断された場合には、コンテンツ利用制御受信装置5にスクランブル鍵Ksが送出され(S52)、このスクランブル鍵Ksを受信したコンテンツ利用制御受信装置5では、コンテンツデスクランブル部15で、暗号化コンテンツが復号される(S53)。

【0113】S51にて、再生手順番号の数値が記憶部Nに記憶されている数値nと同じであると判断されない場合には、再生手順番号の数値が数値n未満か、または再生手順番号の数値が数値nに1加算した値であるかどうか判断される(S54)。再生手順番号の数値が数値n未満か、再生手順番号の数値が数値nに1加算した値であると判断されない場合には、スクランブル鍵Ksの送出が中断され、コンテンツ利用制御受信装置5においてエラー処理が行われる(S55)。このエラー処理はセキュリティモジュールSM1がコンテンツ利用制御受信装置5に対して暗号化コンテンツを復号できない旨のエラー番号(エラー情報)を送出することによって実行される。

【0114】S54にて、再生手順番号の数値が数値n未満か、再生手順番号の数値がnに1加算した値であると判断された場合には、この数値nが記憶部Nに記憶され(S56)、コンテンツ利用制御受信装置5にスクランブル鍵Ksが送出され(S52)、このスクランブル鍵Ksを受信したコンテンツ利用制御受信装置5では、コンテンツデスクランブル部15で、暗号化コンテンツが復号される(S53)。

【0115】これらの動作によれば、デスクランブルしたいコンテンツの、最初に受信された再生手順番号の数値を記憶部Nの初期値として設定しているため、リアルタイムに受信しているコンテンツ(デスクランブルした

いコンテンツ)を途中から視聴したり、コンテンツの冒頭から記憶部17に記憶していないコンテンツの再生が可能になり、再生手順番号に従ったコンテンツの視聴制限(視聴制御)を行うことができる。

【0116】(視聴制御フラグに関して補足)ここまでの説明において、視聴制御フラグをオン・オフのみの1ビットの利用制御情報としてきた。しかし、視聴制御フラグのビット数を増加させて、例えば、視聴制御フラグが0の時は、視聴制御自体をオフ、視聴制御フラグが1の時は図7に示したシーケンスチャートに基づく制御、視聴制御フラグが2の時は、図8に示したシーケンスチャートに基づく制御とすることも可能である。

【0117】この実施の形態では以下の効果を奏す。コンテンツ利用制御送信装置3では、スクランブル鍵Ksを用いて、コンテンツスクランブル部7(7a)でコンテンツが暗号化され暗号化コンテンツとされる。一方、暗号化器7bで、記憶部11に記憶されているコンテンツ鍵Kcによって、少なくとも再生手順番号およびスクランブル鍵Ksを含む関連情報が暗号化し暗号化関連情報とされる。また、暗号化器7cで、記憶部11に記憶されているワーク鍵Kwによって、少なくとも視聴制御フラグおよびコンテンツ鍵Kcを含む当該コンテンツ鍵Kcに関するコンテンツ鍵関連情報が暗号化され暗号化コンテンツ鍵関連情報とされる。さらに、暗号化器7dで、マスター鍵によって、少なくともワーク鍵Kwを含むワーク鍵Kwに関するワーク鍵関連情報が暗号化され暗号化ワーク鍵関連情報とされる。そして、多重化部9で、これらが多重化暗号コンテンツとされ、送信される。

【0118】コンテンツ利用制御受信装置5では、分離部13で、暗号化コンテンツ、暗号化関連情報、暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報が送信側のコンテンツ利用制御送信装置3で多重化された多重化暗号コンテンツが受信され、これらが分離される。そしてまた、ここで分離された暗号化ワーク鍵関連情報がマスター鍵Kmにより復号器15aで復号されワーク鍵Kwが得られ、復号器15bで、得られたワーク鍵Kwで暗号化コンテンツ鍵Kcおよび暗号化されている視聴制御フラグが復号され、コンテンツ鍵Kcおよび視聴制御フラグが得られる。この視聴制御情報フラグに基づいて、復号器15cで、暗号化スクランブル鍵Ksおよび暗号化されている再生手順番号が復号され、この再生手順番号に基づいて、コンテンツデスクランブル部15(15d)にて、スクランブル鍵Ksで暗号化コンテンツが復号され、コンテンツが得られる。

【0119】つまり、コンテンツ利用制御送信装置3およびコンテンツ利用制御受信装置5においてコンテンツの暗号化、復号に、暗号化関連情報(スクランブル鍵関連情報)に含まれている再生手順番号によりグループ化されたスクランブル鍵Ksを用いることで、受信側の受

信機が不正に改造されたり不正に製造されたものであっても、コンテンツの不正利用を防止することができ、さらに送信側の放送局(放送事業者)が、受信側でのコンテンツの視聴順序を指定する、コンテンツの利用制御を実現することができる。

【0120】また、送信側の放送局が設定した再生手順番号(再生順序制御情報)により、あるシーンやCMのスキップを受信側に委ねず、送信側で制御することができ、コンテンツの制作者(放送局(放送事業者))の意図した通りに、受信側でコンテンツを利用させることができる。さらに、CM等の広告収入を主な収入源にしている民間の無料放送事業者は、広告収入を確保しながら、コンテンツのノンリニア再生や、メタデータによるコンテンツ検索等の便利な新サービスを視聴者に提供することができる。

【0121】以上、一実施形態に基づいて本発明を説明したが、本発明はこれに限定されるものではない。コンテンツ利用制御送信装置3、コンテンツ利用制御受信装置5の各構成の処理を、一般的なプログラム言語で記述したコンテンツ送信プログラム、コンテンツ受信プログラムとみなすことも可能である。この場合も、コンテンツ利用制御送信装置3、コンテンツ利用制御受信装置5で得られる効果と同様の効果が得られる。さらに、このプログラムを記憶媒体(フレキシブルディスク、CD-ROM等)に記憶し、流通させることも可能である。

【0122】

【発明の効果】請求項1記載の発明によれば、スクランブル鍵によって暗号化された暗号化コンテンツと、共通鍵によって暗号化された暗号化関連情報とが、多重化ステップにおいて多重化され多重化暗号コンテンツとされ送信される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視するために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除くとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【0123】請求項2記載の発明によれば、利用制御情報が再生順序制御情報と視聴制御情報との少なくとも一方の情報を含んでいるので、受信側でコンテンツを利用するときに、この情報に従って、送信側の意図するようにコンテンツの利用制御を受信側で行わせることができる。

【0124】請求項3記載の発明によれば、スクランブル鍵によって暗号化された暗号化コンテンツと、コンテンツ鍵によって暗号化された暗号化関連情報と、ワーク鍵によって暗号化された暗号化コンテンツ鍵関連情報と、マスター鍵によって暗号化された暗号化ワーク鍵関

連情報が、多重化ステップにおいて多重化され多重化暗号コンテンツとされ送信される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視するために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【0125】請求項4記載の発明によれば、受信された多重化暗号コンテンツが暗号化コンテンツと暗号化関連情報とに分離され、暗号化利用制御情報復号ステップで、暗号化スクランブル鍵および暗号化利用制御情報が復号され、暗号化コンテンツ復号ステップで、復号された利用制御情報に基づいて暗号化コンテンツが復号される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視するために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【0126】請求項5記載の発明によれば、受信された多重化暗号コンテンツが暗号化コンテンツと暗号化関連情報と暗号化コンテンツ鍵関連情報と暗号化ワーク鍵関連情報とに分離され、暗号化ワーク鍵関連情報がマスター鍵で復号され、復号されたワーク鍵で暗号化コンテンツ鍵および暗号化視聴制御情報が復号され、復号された視聴制御情報に基づいて、暗号化スクランブル鍵および暗号化再生順序制御情報が復号され、復号された再生順序制御情報に基づいて、スクランブル鍵で暗号化コンテンツが復号される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視するために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【0127】請求項6記載の発明によれば、スクランブル鍵によって暗号化された暗号化コンテンツと、共通鍵によって暗号化された暗号化関連情報とが、多重化手段において多重化され多重化暗号コンテンツとされ送信される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制

御情報を無視するために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【0128】請求項7記載の発明によれば、利用制御情報が再生順序制御情報と視聴制御情報との少なくとも一方の情報を含んでいるので、受信側でコンテンツを利用するときに、この情報に従って、送信側の意図するようにコンテンツの利用制御を受信側で行わせることができる。

【0129】請求項8記載の発明によれば、スクランブル鍵によって暗号化された暗号化コンテンツと、コンテンツ鍵によって暗号化された暗号化関連情報と、ワーク鍵によって暗号化された暗号化コンテンツ鍵関連情報と、マスター鍵によって暗号化された暗号化ワーク鍵関連情報が、多重化手段において多重化され多重化暗号コンテンツとされ送信される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視するために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【0130】請求項9記載の発明によれば、受信された多重化暗号コンテンツが暗号化コンテンツと暗号化関連情報とに分離され、暗号化利用制御情報復号手段で、暗号化スクランブル鍵および暗号化利用制御情報が復号され、暗号化コンテンツ復号手段で、復号された利用制御情報に基づいて暗号化コンテンツが復号される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視するために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【0131】請求項10記載の発明によれば、受信された多重化暗号コンテンツが暗号化コンテンツと暗号化関連情報と暗号化コンテンツ鍵関連情報と暗号化ワーク鍵関連情報とに分離され、暗号化ワーク鍵関連情報がマスター鍵で復号され、復号されたワーク鍵で暗号化コンテンツ鍵および暗号化視聴制御情報が復号され、復号された視聴制御情報に基づいて、暗号化スクランブル鍵および暗号化再生順序制御情報が復号され、復号された再生順序制御情報に基づいて、スクランブル鍵で暗号化コン

テンツが復号される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視にするために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【0132】請求項11記載の発明によれば、コンテンツ利用制御送信プログラムにおいて、スクランブル鍵によって暗号化された暗号化コンテンツと、共通鍵によって暗号化された暗号化関連情報とが、多重化手段において多重化され多重化暗号コンテンツとされ送信される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視にするために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【0133】請求項12記載の発明によれば、コンテンツ利用制御送信プログラムにおいて、利用制御情報が再生順序制御情報と視聴制御情報との少なくとも一方の情報を含んでいるので、受信側でコンテンツを利用するときに、この情報に従って、送信側の意図するようにコンテンツの利用制御を受信側で行わせることができる。

【0134】請求項13記載の発明によれば、コンテンツ利用制御送信プログラムにおいて、スクランブル鍵によって暗号化された暗号化コンテンツと、コンテンツ鍵によって暗号化された暗号化関連情報と、ワーク鍵によって暗号化された暗号化コンテンツ鍵関連情報と、マスター鍵によって暗号化された暗号化ワーク鍵関連情報が、多重化手段において多重化され多重化暗号コンテンツとされ送信される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視にするために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【0135】請求項14記載の発明によれば、コンテンツ利用制御受信プログラムにおいて、受信された多重化暗号コンテンツが暗号化コンテンツと暗号化関連情報とに分離され、暗号化利用制御情報復号手段で、暗号化スクランブル鍵および暗号化利用制御情報が復号され、暗

号化コンテンツ復号手段で、復号された利用制御情報に基づいて暗号化コンテンツが復号される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視にするために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【0136】請求項15記載の発明によれば、コンテンツ利用制御受信プログラムにおいて、受信された多重化暗号コンテンツが暗号化コンテンツと暗号化関連情報と暗号化コンテンツ鍵関連情報と暗号化ワーク鍵関連情報とに分離され、暗号化ワーク鍵関連情報がマスター鍵で復号され、復号されたワーク鍵で暗号化コンテンツ鍵および暗号化視聴制御情報が復号され、復号された視聴制御情報に基づいて、暗号化スクランブル鍵および暗号化再生順序制御情報が復号され、復号された再生順序制御情報に基づいて、スクランブル鍵で暗号化コンテンツが復号される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視にするために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【図面の簡単な説明】

【図1】本発明による一実施の形態であるコンテンツ利用制御システム（コンテンツ利用制御送信装置およびコンテンツ利用制御受信装置）のブロック図である。

【図2】コンテンツ利用制御送信装置から送信されるファイルのフォーマット例を説明した説明図である。

【図3】コンテンツ利用制御受信装置およびセキュリティモジュールを説明した説明図である。

【図4】コンテンツに付されている再生手順番号に基づいたコンテンツの視聴制御（視聴制御フラグオン）を説明した説明図である。

【図5】コンテンツに付されている再生手順番号に基づいたコンテンツの視聴制御（視聴制御フラグオフ）を説明した説明図である。

【図6】コンテンツ利用制御受信装置でコンテンツを視聴制御する際の動作（記憶後、ノンリニア再生）を説明したシーケンスチャートである。

【図7】コンテンツ利用制御受信装置でコンテンツを視聴制御する際の動作（記憶後、再生手順番号順）を説明したシーケンスチャートである。

【図8】コンテンツ利用制御受信装置でコンテンツを視

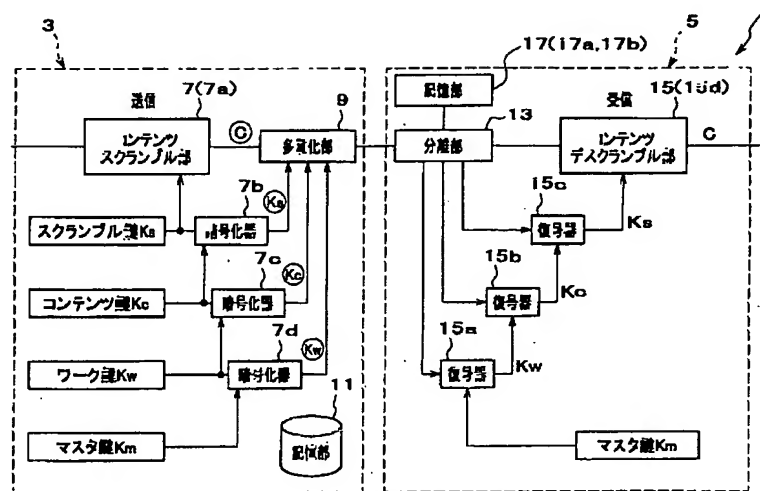
聴制御する際の動作（リアルタイム）を説明したシーケンスチャートである。

【符号の説明】

- 1 コンテンツ利用制御システム
- 3 コンテンツ利用制御送信装置
- 5 コンテンツ利用制御受信装置

- 7 コンテンツスクランブル部
- 9 多重化部
- 11、17 記憶部
- 13 分離部
- 15 コンテンツデスクランブル部

【図1】



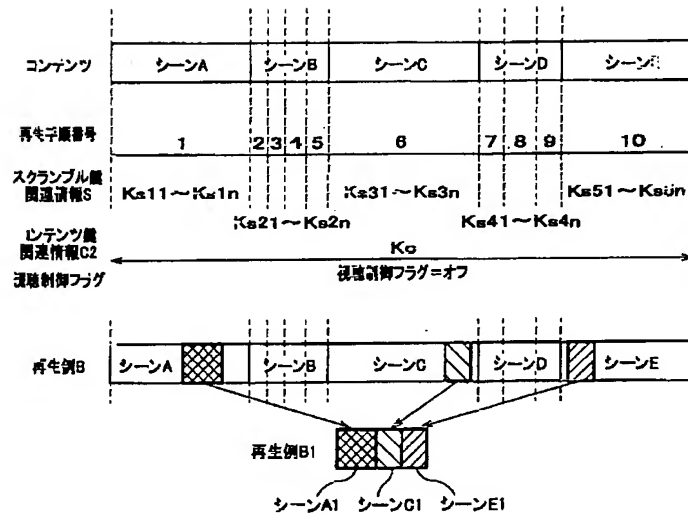
※ ○で囲まれた記号は、暗号化されていることを示している。

【図2】

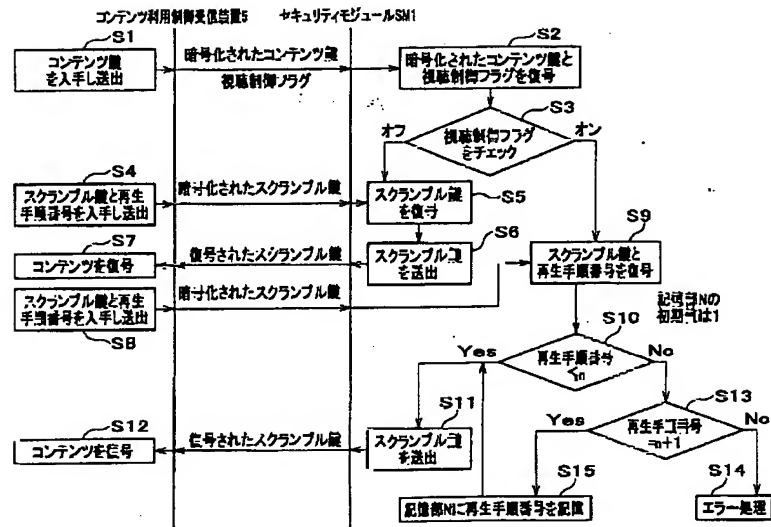
スクランブル鍵関連情報S	コンテンツ鍵関連情報C	ワーク鍵関連情報W
事業者ID コンテンツID スクランブル鍵Ks 再生手続番号	事業者ID ワークID コンテンツID コンテンツ鍵Kc 有効期限 管理場所指定 視聴制御フラグ	事業者ID カードID 更新番号 有効期限 ワークID ワーク鍵Kw



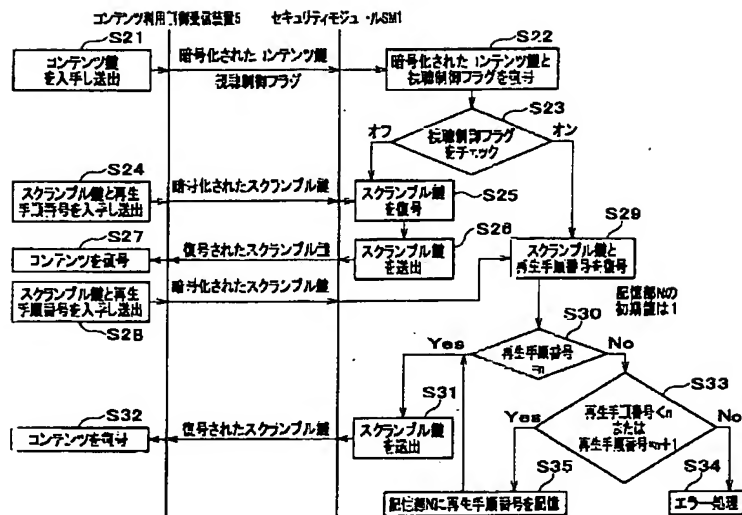
【図5】



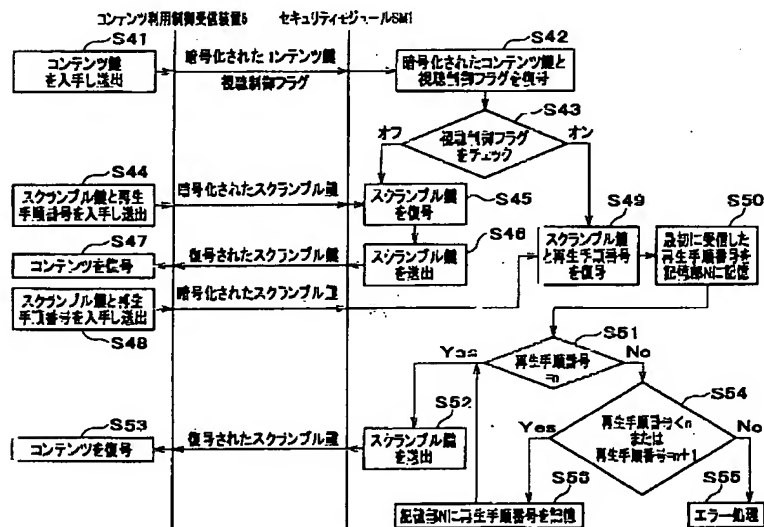
【図6】



【図7】



【図8】



フロントページの続き

(51) Int. Cl.⁷

識別記号

F I

(参考)

H 0 4 N 7/167

(72) 発明者 上原 年博

東京都世田谷区砧一丁目10番11号 日本放
送協会 放送技術研究所内

(72) 発明者 難波 誠一

東京都世田谷区砧一丁目10番11号 日本放
送協会 放送技術研究所内

(26) 03-152698 (P2003-152698A)

(72)発明者 奥田 治雄

東京都世田谷区砧一丁目10番11号 日本放
送協会 放送技術研究所内

Fターム(参考) 5C063 AB03 AB11 DA13 DA20

5C064 BC22 BC25 CA14 CB01 CC04

5J104 AA16 BA03 EA07 EA18 NA02

NA03 PA05

【発明の名称】

コンテンツ利用制御送信方法、コンテンツ利用制御受信方法およびコンテンツ利用制御送信装
置、コンテンツ利用制御受信装置ならびにコンテンツ利用制御送信プログラム、コンテンツ利用
制御受信プログラム

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.